高等教育质量工程信息技术系列示范教材

信息系统安全教程

（第3版）习题详解

栾英姿 王玉斐 编著

清华大学出版社

高等教育质量工程信息技术系列示范教材

信息系统安全教程（第3版）习题详解

栾英姿 王玉斐 编著

清华大学出版社
北京

内 容 简 介

为了配合信息系统安全课程的教学，以及广大管理技术人员对于信息安全的系统学习，本书解答了张基温教授编写的《信息系统安全教程》第 3 版的全部习题，并附加 2017 年信息系统安全课程的考卷及答案两份。本书主体部分为 5 章，分别对应原教材的 5 章内容，即信息系统安全威胁、数据安全保护、身份认证与访问控制、网络安全保护和信息系统安全管理。

本书结合实际案例和当前网络中的常见问题，从宏观角度系统阐述信息系统安全管理和防御的基本策略，在细节上紧扣现代生产生活中的应用热点，引导读者正确看待网络安全防御策略，进一步做好安全规划和管理。书中配有实际案例，对容易引起混淆的概念进行了简明分析，是学习信息系统安全的基础教材。适合作为信息安全、网络安全、通信安全、计算机网络、信息管理等专业“信息系统安全”课程的教学参考书，也可供相关专业技术管理人员参考。

图书在版编目（CIP）数据

信息系统安全教程（第 3 版）习题详解 / 栾英姿，王玉斐编著. —3 版. —北京：清华大学出版社，2019
（高等教育质量工程信息技术系列示范教材）
ISBN 978-7-302-51743-6

Ⅰ. ①信…　Ⅱ. ①栾…　②王…　Ⅲ. ①信息系统－安全技术－高等学校－题解　Ⅳ. ①TP309－44

中国版本图书馆 CIP 数据核字（2018）第 271368 号

责任编辑： 白立军　常建丽
封面设计： 常雪影
责任校对： 时翠兰
责任印制： 沈　露

出版发行： 清华大学出版社
网　　址：http://www.tup.com.cn, http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　编：100084
社 总 机：010-62770175　　邮　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn,010-62795954
印 装 者： 北京国马印刷厂
经　　销： 全国新华书店
开　　本： 185mm×260mm　　印　张：9.5　　字　数：223 千字
版　　次： 2007 年 8 月第 1 版　　2019 年 6 月第 3 版　　印　次：2019 年 6 月第 1 次印刷
定　　价： 29.00 元

产品编号：075147-01

前　言

随着有线和无线信息系统的快速发展，网络安全问题成为21世纪最重要的研究课题之一。计算机网络的最初形成和发展来自于海外国家，我国在紧跟国际发展的基础上，又开拓了很多新的领域和新的应用。对于网络安全的研究，既要吸收采纳国外的相关先进理论、技术和产品，也要迅速发展国内的研究能力。近十几年出现了一大批计算机网络安全方面的优秀教材，而对于教材中对学子们提出的问题，也需要精确全面的解答，以引导整个领域更加蓬勃健康地发展。本书正是在此大背景下应运而生。

网络安全涉及的领域很广，包括设备供应商、网络服务商、网络管理层、计算机用户等多方面的需求，黑客的恶意攻击和用户的懈于防护使得网络诈骗、网络病毒、网络瘫痪出现的概率越来越大，对于网络信息安全需要各个层面的重视。

习近平总书记在2018年中国国际大数据产业博览会5月26日的开幕式贺信中提到，要建设网络强国、数字中国、智慧社会，并在多次讲话中提到要形成党委领导、政府管理、企业履责、社会监督、网民自律等多主体参与，经济、法律、技术等多种手段相结合的综合治网格局。要加强网上正面宣传，积极培育和践行社会主义核心价值观。

《孙子兵法》中说：知己知彼，百战不殆；不知彼而知己，一胜一负；不知彼不知己，每战必殆。因此，要成为信息安全防御方面的能手，必须深入了解攻击者惯于使用的伎俩，并且建立长期有效的防御体制，才能确保整个通信系统的安全。

本习题详解基本概括了当前网络中存在的各种干扰不安全因素，并阐明了防御方案。第1章习题囊括了病毒、木马、蠕虫、窃听、扫描攻击、IP欺骗、路由欺骗、TCP会话劫持、DNS欺骗、Web欺骗、邮件欺骗、伪基站攻击、缓冲区溢出、拒绝服务攻击等计算机信息系统中过去几十年危害网络的常用攻击手法以及防御措施；第2章习题主要涉及加密算法、数据完整性和真实性保护；第3章习题包括数字签名、身份认证、访问控制等国际标准的相关知识和内容；第4章习题涉及防火墙、网络隔离、Internet安全协议，包括IPSec、SSL、VPN等，以及对于入侵检测技术和蜜罐技术的阐述和解答；第5章习题涉及信息系统安全管理层面，包括应急响应、风险评估方面比较成熟的方案介绍。附录中给出了两套综合试题及其解答，以便于阅读者自学。

本书第1～4章习题解答由栾英姿编写，第5章习题解答由王玉斐编写。在整个编写过程中，得到清华大学出版社各位领导、同事的支持和认可，原教材作者张基温教授也一直密切关注和指导本书的写作，在此一并致谢，感恩！

栾英姿

2019年2月

目　　录

第 1 章　信息系统安全威胁

1.1　第 1 章知识提要

本章详细讲解了蠕虫、病毒、特洛伊木马等恶意代码的各自特点，以及后门、扫描、监听等技术；对传统窃听技术，包括声波、电磁波、光缆窃听以及手机监听的要点，进行了解答和分析；对网络欺骗的分类，包括 ARP 欺骗、IP 欺骗、路由欺骗、会话劫持、重放攻击、DNS 欺骗、Web 欺骗和伪基站攻击等关键问题进行了解答；对黑客常用的攻击方法、缓冲区溢出、拒绝服务攻击等进行了原理阐述。

1.2　第 1 章习题和答案详解

一、选择题（答案：BBCBD BBCAC AABAA EABBD）

1. 下列关于计算机病毒的叙述中，________是错误的。
   A. 计算机病毒会对计算机文件和数据造成破坏
   B. 只要删除感染了病毒的文件，就可以彻底清除病毒
   C. 计算机病毒是一段人为制造的小程序
   D. 计算机病毒是可以预防和清除的

答案：B

解答： 计算机病毒的特点是隐藏性、传染性、繁殖性，仅通过清除一个文件是很难彻底清除影响的。

2. 计算机病毒是指“能够侵入计算机系统并在计算机系统中破坏系统正常工作的一种具有繁殖能力的________”。
   A. 一种被破坏了的程序
   B. 具有破坏性，并可以在计算机中潜伏、传播的特殊小程序
   C. 特殊微生物
   D. 源程序

答案：B

解答： 根据计算及病毒的定义可以知道：计算机病毒（computer virus）是编制者在计算机程序中插入的破坏计算机功能或者数据代码，能影响计算机使用，能自我复制的一组计算机指令或者程序代码。它的特点是传播性、隐蔽性、感染性、潜伏性、可激发性、表现性和破坏性。

3. 下列关于计算机病毒的说法中，正确的是________。

A. 计算机病毒是一种有损计算机操作人员身体健康的生物病毒

B. 当U盘或光盘不清洁时，将会传播计算机病毒

C. 计算机病毒是一种通过自我复制进行传染的，破坏计算机程序和数据的小程序

D. 计算机病毒是一种有逻辑错误的程序

答案：C

解答：计算机病毒不是生物病毒，不是物理病毒，也没有逻辑错误。

4. 防止U盘感染病毒的有效方法是________。

A. 不要把无毒U盘与有毒U盘放在一起

B. 使U盘写保护

C. 保持机房清洁

D. 定期用酒精对U盘进行消毒

答案：B

解答：由于计算机病毒的非物理性，因此其他选项都不对，只有B正确。

5. 计算机宏病毒主要感染________文件。

A. .exe

B. .com

C. .txt

D. .doc

答案：D

解答：宏病毒是一种寄存在文档或模板的宏中的计算机病毒。一旦打开这样的文档，其中的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在Normal模板上。至此，所有自动保存的文档都会“感染”上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上，因此它只感染.doc文档。

6. 计算机病毒最重要的特点是________。

A. 可执行

B. 可传染

C. 可保存

D. 可打印

答案：B

解答：计算机病毒最重要的特性是传染性。

7. 为了预防计算机病毒，应采取的正确措施是________。

A. 每天都对计算机硬盘和软件进行格式化

B. 不用盗版软件和来历不明的软盘

C. 不与任何人交流
D. 不玩任何计算机游戏

答案：B

解答：因为计算机病毒容易隐藏在盗版软件或来历不明的软盘中。所以选B。

8. 下列描述中，不属于引导扇区病毒的是________。
A. 用自己的代码代替MBR中的代码
B. 会在操作系统之前加载到内存中
C. 将自己复制到计算机的每个磁盘
D. 格式化硬盘

答案：C

解答：引导区病毒是指病毒寄存在硬盘主引导区所占据的0面第一扇区中，因此选C。

9. 特洛伊木马________。
A. 表面上看起来无害，但隐藏着罪恶
B. 不是有意破坏，仅制造恶作剧
C. 经常将自己复制，附着在宿主文件中
D. 传播和运行都不需要客户参与

答案：A

解答：特洛伊木马的特点是伪装成一个实用工具、一个可爱的游戏、图片、软件，诱使用户将其安装在PC端或者服务器上，从而秘密获取信息。

10. 蠕虫________。
A. 不进行自我复制
B. 不向其他计算机传播
C. 不需要宿主文件
D. 不携带有效负载

答案：C

解答：蠕虫的特点是独立、自主、传播、有害，所以选C。

11. 后门________。
A. 是为计算机系统开启秘密访问入口的程序
B. 会大量占用计算机资源，造成计算机瘫痪
C. 用于对互联网中的目标主机发起攻击
D. 用于寻找电子邮件地址，发送垃圾邮件

答案：A

解答：后门程序一般是指那些绕过安全性控制获取对程序或系统访问权的程序方法。在软件开发阶段，程序员常会在软件内创建后门程序，以方便修改程序设计中的缺陷。

但是，如果这些后门被其他人知道，或是在发布软件之前没有删除后门程序，那么它就成了安全风险，容易被黑客当成漏洞进行攻击，所以选A。

12. 从安全属性对各种网络攻击进行分类，截获攻击是针对________的攻击。

A. 机密性

B. 可用性

C. 完整性

D. 真实性

答案：A

解答：截获攻击与保密性相关，伪造攻击与认证相关，篡改攻击与完整性相关，中断攻击与可用性相关，所以选A。

13. “会话侦听和劫持技术”是属于________技术。

A. 密码分析还原

B. 协议漏洞渗透

C. 应用漏洞分析与渗透

D. DOS攻击

答案：B

解答：会话劫持（session hijack）是一种结合了嗅探及欺骗技术在内的攻击手段，它利用TCP/IP的漏洞得以实现，因此选B。

14. 攻击者用传输数据冲击网络接口，使服务器过于繁忙，以至于不能应答请求的攻击方式是________。

A. 拒绝服务攻击

B. 地址欺骗攻击

C. 会话劫持

D. 信号包探测程序攻击

答案：A

解答：只有拒绝服务攻击最符合题中的描述，因此选A。

15. 攻击者截获并记录了从A到B的数据，然后从所截获的数据中提取出信息重新发往B，这种攻击称为________。

A. 中间人攻击

B. 口令猜测器和字典攻击

C. 强力攻击

D. 回放攻击

答案：A

解答：一般回放攻击指的是经过加密的口令被截获后无法解密只能以密文形式再次回放以

达到欺骗身份认证的目的，而中间人攻击是指中间人监听到A、B之间的通信，通过ARP欺骗冒充某一方和另一方进行通信，因此A更符合题中的描述。

16. 拒绝服务攻击的后果是________。
   A. 系统不可用
   B. 应用程序不可用
   C. 系统死机
   D. 阻止通信
   E. 上面几项都是

答案：E

解答：拒绝服务攻击造成的后果有系统不可用、应用程序不可用、系统死机、阻止通信，因此选E。

17. DDoS攻击破坏了信息的________。
   A. 可用性
   B. 保密性
   C. 完整性
   D. 真实性

答案：A

解答：分布式拒绝服务（DDoS）攻击造成系统不可用，因此选A。

18. 某用户收到一封可疑的电子邮件，要求他提供银行账户及密码。这是一种________攻击手段。
   A. 缓存溢出
   B. 钓鱼
   C. 后门
   D. DDoS

答案：B

解答：钓鱼攻击手段就是使用骗取用户信任的方法取得用户名和密码，只有答案B满足要求。

19. 在网络攻击中，攻击者窃取到系统的访问权并盗用资源进行的攻击属于________。
   A. 拒绝服务
   B. 侵入攻击
   C. 信息盗窃
   D. 信息篡改

答案：B

解答：侵入攻击符合题中的描述。A、C、D都不符合或不完全符合题中的描述，因此选B。

20. 下列关于特征和行为的描述中，不属于DoS的是________。

A. 利用操作系统或应用系统的薄弱环节发起攻击

B. 生成足够多的业务量拖垮服务器

C. 对计算机系统资源进行极大的占用

D. 使用电子邮件地址列表向其他计算机发送自己的副本

答案：D

解答：只有D不属于拒绝服务攻击（DoS）的特征和行为。

二、填空题

答案：1. 破坏计算机数据并影响计算机正常工作的，合法程序

2. 可触发性，非授权执行性

3. 一段具有破坏性的程序代码，计算机系统内部

4. 蠕虫病毒

5. 漏洞扫描

6. 集中式，分布式

1. 计算机病毒是一段 破坏计算机数据并影响计算机正常工作的 程序，它不单独存在，经常是附属在 合法程序 的起、末端，或磁盘引导区、分配表等存储器件中。
2. 计算机病毒的5个特征是：主动传染性、破坏性、可触发性、寄生性（隐蔽性）和 非授权执行性。
3. 计算机病毒是一段具有破坏性的程序代码，它能够侵入计算机系统内部，并且能够通过修改其他程序，把自己或者自己的变种复制插入其他程序中；这些程序又可传染别的程序，实现繁殖传播。
4. 蠕虫病毒是一组计算机指令或者程序代码，能自我复制，通常嵌入在计算机程序中，能够破坏计算机功能或者毁坏数据，影响计算机的使用。
5. 漏洞扫描是对计算机系统或其他网络设备进行与安全相关的检测，找出安全隐患和可被黑客利用的漏洞。
6. DDos的攻击形式主要有集中式 和 分布式。

三、问答题

1. 举一例说明你所遇到的信息系统安全威胁事件。

答：2015 年底，我的一个在国外访学的同事 QQ 账户被盗，有一个人冒充他和我聊天，要我给相关部门寄 1800 元钱，后来通过核实是一场骗局。这是他的 QQ 密码被黑客破解引起的安全威胁事件。

2. 什么是 0day 漏洞？

答：0day 漏洞又称零日漏洞，是指在操作系统安全补丁发布前被黑客了解和掌握的漏洞信息。

3. 收集充分的证据，论述病毒程序的特征。

答：病毒程序的五个特征为：传染性，破坏性，非授权执行性，隐蔽性（寄生性），可触发性。

（1）传染性：正常的计算机程序一般是不会将自身的代码强行连接到其他程序之上的。而病毒却能使自身的代码强行传染到一切符合其传染条件的未受到传染的程序上。计算机病毒可通过各种可能的渠道，如软盘、计算机网络等传染其他的计算机。当您在一台机器上发现了病毒时，往往曾在这台计算机上用过的软盘已感染上病毒，而与这台机器相联网的其他计算机也许已被该病毒染上了。是否具有传染性是判别一个程序是否为计算机病毒的最重要的条件。

（2）破坏性：所有的计算机病毒都存在一个共同的危害，即降低计算机系统的工作效率，占用系统资源，其具体情况取决于入侵系统的病毒程序。同时，计算机病毒的破坏性主要取决于计算机病毒设计者的目的，如果病毒设计者的目的在于彻底破坏系统的正常运行，那么这种病毒对计算机系统进行攻击造成的后果是难以设想的，它可以毁掉系统的部分数据，也可以破坏全部数据并使之无法恢复。

（3）非授权执行性：病毒未经授权而执行。一般正常的程序由用户调用，再由系统分配资源，完成用户交给的任务。其目的对用户是可见的、透明的。而病毒具有正常程序的一切特性，它隐藏在正常程序中，当用户调用正常程序时窃取到系统的控制权，先于正常程序执行，病毒的动作、目的对用户是未知的，是未经用户允许的。

（4）隐蔽性：病毒一般是具有很高编程技巧且短小精悍的程序，通常附在正常程序中或磁盘较隐蔽的地方，也有个别的以隐含文件形式出现，目的是不让用户发现它的存在。如果不经过代码分析，病毒程序与正常程序是不容易被区别的。一般在没有防护措施的情况下，计算机病毒程序取得系统控制权后可以在很短的时间里传染大量程序。而且受到传染后，计算机系统通常仍能正常运行，使用户不会感到任何异常，好像不曾在计算机内发生过什么。试想，如果病毒在传染到计算机上之后，机器马上无法正常运行，那么它本身便无法继续进行传染了。正是由于隐蔽性，计算机病毒才得以在用户没有察觉的情况下扩散并游荡于世界上百万台计算机中。大部分病毒的代码之所以设计得非常短小，也是为了隐藏。病毒一般只有几百或 1KB，而 PC 对 DOS 文件的存取速度可达每秒几百 KB 以上，所以病毒转瞬之间便可将这短短的几百字节附着到正常程序中，使人不易察觉。

（5）可触发性：因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性称为可触发性。为了隐蔽自己，病毒必须潜伏，少做动作。如果完全不动，一直潜伏，病毒既不能感染，也不能进行破坏，便失去了杀伤力。病毒既要隐蔽，又要维持杀伤力，它必须具有可触发性。病毒的触发机制是用来控制感染和破坏动作的频率的。病毒具有预定的触发条件，这些条件可能是时间、日期、文件类型或某些特定数据等。病毒运行时，触发机制检查预定条件是否满足，如果满足，就启动感染或破坏动作，使病毒进行感染或攻击；如果不满足，就使病毒继续潜伏。

4. 收集资料，解析下列恶意代码的关键技术。

（1）“求职信”病毒。

（2）“主页”病毒。

（3）“欢乐时光”病毒。

（4）“爱虫”病毒。

（5）“美丽杀”病毒。

（6）“万花谷”病毒。

（7）“红色代码”病毒。

答：（1）“求职信”病毒。“求职信”这种邮件病毒属于黑客木马型邮件病毒，采用双层加密技术，其基本可分为两部分：一部分是狭义上的病毒，它感染 PE 结构文件，病毒大小约为 3KB，用汇编语言编写；第二部分是蠕虫，大小为 56KB，它在运行中会释放并运行一个 11722B 的带毒的 PE 文件。第二部分是用 VC++编写的，它只可在 Windows 9X 或 Windows 2000 上运行，在 NT4 上无法运行。该病毒利用微软系统的漏洞可以自动感染，无须打开附件。

（2）“主页”病毒。“主页”病毒和前不久流行的“库尔尼科娃”病毒很类似，当银行、电话公司、政府机构的工作人员打开含有病毒的电子邮件时，病毒将它们指引到一个色情网站（共有 4 个类似网页）。邮件以 Homepage 为主题，其中所含简短信息如下：“嗨！你应该看看这个网页！真的很酷。”一旦用户打开名为 Homepage.HTML.vbs 的附件，就激活了病毒。接着，病毒就会向中毒机器电子邮件地址簿中的各个用户发出大量邮件，从而导致一些机构的邮件系统陷入瘫痪，无法正常发送邮件。

（3）“欢乐时光”病毒。“欢乐时光”（VBS.Haptime.A@mm）是一个 VB 源程序病毒，专门感染 .htm、.html、.vbs、.asp 和.htt 文件。它作为电子邮件的附件，并利用 Outlook Express 的性能缺陷把自己传播出去。一个被人们所知的 Microsoft Outlook Express 的安全漏洞可以在你没有运行任何附件时就运行自己；还利用 Outlook Express 的信纸功能使自己复制在信纸的 HTML 模板上以便传播。它结合了蠕虫特性和在用户不直接打开情况下直接运行特性，同时能够感染本地的网页及脚本文件。

（4）“爱虫”病毒。这个病毒是通过 Microsoft Outlook 电子邮件系统传播的，邮件的主题为 ILOVEYOU，并包含一个附件。一旦在 Microsoft Outlook 里打开这个邮件，系统就会自动复制并向地址簿中的所有邮件地址发送这个病毒。“我爱你”病毒又称“爱虫”病毒，是一种蠕虫病毒，它与 1999 年的梅丽莎病毒非常相似。据称，这个病毒可以改写本地及网络硬盘上面的某些文件。用户机器感染病毒以后，邮件系统将会变慢，并可能导致整个网络系统崩溃。

（5）“美丽杀”病毒，即 Melissa 病毒，是一种快速传播的能够感染使用 Microsoft Word 97 和 Microsoft Office 2000 的计算机宏病毒。病毒通过 E-mail 传播，传播速度非常快，从 1999 年 3 月 26 日首次被发现到 3 月 29 日，它已经到达 100000 多台计算机。一些站点不得不让它们的主系统离线。据某站点称，它们的系统在 45 分钟之内就收到 32000 份包括 Melissa 病毒的邮件信息副本。

Melissa 病毒通常以 Important Message From……（来自……的重要信息）为主题。从表

面上看，像是熟人或朋友发来的邮件。邮件的正文上写道：Here is the message you asked for…don't tell anyone else;"（这是你向我要的那份文件……不要让别人看到）。邮件的附件是一个 Word 文档。如果收到邮件的人打开了这个文档，病毒就会窜入他的电子通讯簿中，选择最前面的 50 人将染有病毒的邮件发出。

（6）"万花谷"病毒。该病毒是一个比较有代表性的恶意代码网页病毒，在一个叫"万花谷"的网站传出，这是利用 Java 最新技术进行破坏的一个恶意代码。

该病毒的 JS/On888 是一个新的含有有害代码的 ActiveX 网页文件，它通过一个网络地址对计算机用户造成破坏，其破坏特性如下：①用户不能正常使用 Windows 的 DOS 功能程序。②用户不能正常退出 Windows；③开始菜单上的"关闭系统""运行"等栏目被屏蔽，防止用户重新以 DOS 方式启动，关闭 DOS 命令、关闭 REGEDIT 命令等。④IE 浏览器的首页和收藏夹中都加入了含有该有害网页代码的网络地址。

（7）"红色代码"病毒。"红色代码"病毒是一种新型网络病毒，其传播使用的技术可以充分体现网络时代网络安全与病毒的巧妙结合，将网络蠕虫、计算机病毒、木马程序合为一体，开创了网络病毒传播的新路，可称之为划时代的病毒。

该蠕虫感染运行 Microsoft Index Server 2.0 的系统，或是在 Windows 2000、IIS 中启用了 indexing service（索引服务）的系统。该蠕虫利用了一个缓冲区溢出漏洞进行传播（未加限制的 Index Server ISAPI Extension 缓冲区使 Web 服务器变得不安全）。蠕虫只存在于内存中，并不向硬盘复制文件。

蠕虫的传播是通过 TCP/IP 和端口 80，利用上述漏洞，蠕虫将自己作为一个 TCP/IP 流直接发送到染毒系统的缓冲区，蠕虫依次扫描 Web，以便能够感染其他系统。一旦感染了当前的系统，蠕虫就会检测硬盘中是否存在 notworm，如果该文件存在，蠕虫将停止感染其他主机。

5. 在什么情况下，病毒能感染被写保护的文件？

答：举例来说，Windows XP Embedded 产品对系统盘进行写保护，如果对写保护的磁盘进行病毒感染需要改变系统的某些设置，就需要把磁盘写保护改为 Disable 状态，操作如下。

（1）在 Start 中运行 Run 菜单，在 Run 的 Open 栏目中输入 CMD 后单击 OK 按钮，进入命令行状态。

（2）执行 ewfmgr c: 命令查看 State 栏的 EWF 状态，若是 Enable 状态，则可在命令行下执行 ewfmgr-commitanddisable c: 命令，将磁盘写保护改为 Disable 状态。

（3）重新启动计算机，确认磁盘写保护为 Disable 状态，此时病毒就可以感染磁盘了。对于受写保护的文件执行病毒感染，方法与上类似。

6. 收集资料，解析一种最新病毒的关键技术。

答：2017 年 5 月 13 日，勒索病毒（WannaCry）在全球蔓延，据不完全统计，目前已经入侵 99 个国家 7.5 万台计算机，其中中国高校受到的伤害最严重，而这给学生们带来的打击也是超级大的，毕竟已经是论文季了。该勒索蠕虫一旦攻击进入能连接公网的用户机

器，则会扫描内网和公网的 IP，若被扫描到的 IP 打开了 445 端口，则会使用 EternalBlue（永恒之蓝）漏洞安装后门。一旦执行后门，则会释放一个名为 Wana Cryptor 敲诈者病毒，从而加密用户机器上所有的文档文件进行勒索。病毒导致计算机内的文件无法打开，除非支付一定的比特币。勒索软件采用的是 RSA + AES 加密算法加密文件，属于几乎无法在有限时间内破解的加密算法。主流的勒索病毒通常有两种文件操作方式：一种是直接加密覆盖原文件，这种情况下没有勒索者的密钥，几乎是无法恢复的；另一种则是先加密生成副本文件，然后删除原文件，这种情况下是有可能恢复的。

7. 总结现代病毒技术及其发展趋势。

答：现代病毒技术有以下五个特点。

（1）病毒变种繁多，演化日趋完善。

（2）混合通用型病毒。

（3）隐藏型病毒。

（4）多态型病毒。

（5）病毒的自动化生产。

现代计算机病毒的发展趋势仍然是隐蔽性和非授权性，并在短时间内大量传播。由于用户对网络的高度信赖，经常下载软件，单击不明插件，光顾富有吸引力的小网站，导致计算机病毒很容易入侵计算机。另外，用户在实际应用中也会经常启动在线阅读，而不知部分计算机网络病毒隐藏在文件中，导致病毒传播率增长迅猛。

8. 讨论现代病毒检测技术的发展趋势。

答：按照先后发展顺序可分为：

（1）用静态广谱特征扫描方式检测病毒。

（2）将静态扫描技术和动态仿真跟踪技术结合起来，将查找病毒和清除病毒合二为一，形成一个整体解决方案针对计算机病毒的发展。

（3）基于病毒家族体系的命名规则、CRC 校验和扫描机理，采用启发式智能代码分析模块、动态数据还原模块（能查出隐藏性极强的压缩加密文件中的病毒）、内存杀毒模块、自身免疫模块等先进检测方法检测病毒。

9. 讨论现代反病毒技术的发展趋势。

答：第一代反病毒技术是单纯地基于病毒特征判断，直接将病毒代码从带毒文件中删除。这种方式可以准确地清除病毒，可靠性很高。后来病毒技术的发展，特别是加密和变形技术的运用，使得这种简单的静态扫描方式失去作用。

第二代反病毒技术是采用静态广谱特征扫描方式检测病毒。这种方式可以更多地检测出变形病毒，但误报率也很高，尤其是用这种不严格的特征判定方式清除病毒带来的风险性很大，容易造成文件和数据的破坏。所以，静态防病毒技术也有难以克服的缺陷。

第三代反病毒技术的主要特点是将静态扫描技术和动态仿真跟踪技术结合起来，将查找病毒和清除病毒合二为一，形成一个整体解决方案，能够全面实现防、查、杀等反病毒

所必备的手段，以驻留内存的方式检测病毒的入侵，凡是检测到的病毒都能清除，不会破坏文件和数据。随着病毒数量的增加和新型病毒技术的发展，静态扫描技术将会使查毒软件速度降低，驻留内存防病毒模块也容易产生误报。

第四代反病毒技术则是针对计算机病毒的发展，基于病毒家族体系的命名规则、CRC 校验和扫描机理，具备启发式智能代码分析模块、动态数据还原模块（能查出隐藏性极强的压缩加密文件中的病毒）、内存杀毒模块、自身免疫模块等先进杀毒方法的反病毒技术。它较好地解决了以前防病毒技术顾此失彼、此消彼长的状况。

10. 收集资料，讨论针对当前 3 种流行病毒的查、杀和感染后的恢复方法。

答：举例来说，鬼影病毒是当之无愧的 2012 年度毒王，它主要依靠带毒游戏外挂或色播传播，2012 年内出现数个变种，包括鬼影 5、鬼影 6、鬼影 6 变种(CF 三尸蛊)等，它和杀毒软件的技术对抗也达到了一个新的高度。经常下载使用带毒游戏外挂的计算机用户是感染鬼影病毒的高危群体。

可以采用主流的杀毒软件查杀鬼影病毒。由于鬼影病毒并不破坏文件，计算机中的文件不会被破坏或者感染，所以可以把计算机中的原有重要文件提前复制出来。另外，鬼影病毒感染的是引导区，所以需要使用工具恢复引导区后再使用杀毒软件杀毒。或者全盘格式化计算机，重新分区，重写 MBR（主引导记录），然后重装系统也可以解决鬼影病毒的感染问题。其他病毒及查杀和感染后的恢复方法，读者可以自行查阅相关网页内容。

11. 收集资料，讨论针对当前 3 种流行蠕虫的查、杀和感染后的恢复方法。

答：1）勒索病毒

2017 年 5 月 12 日，黑客借助由美国国家安全局泄露出的漏洞攻击工具，利用高危漏洞 EternalBlue(永恒之蓝)在世界范围内传播 WannaCry 勒索病毒，致使 WannaCry 勒索病毒大爆发。据相关报道，包括俄罗斯、美国、英国、中国等在内的 150 多个国家、地区近 30 万台设备均受到其攻击。其影响涉及教育、金融、能源和医疗等众多行业，英国国家医疗服务体系遭遇了大规模网络攻击，多家公立医院的计算机系统几乎同时瘫痪，电话线路也被切断，导致很多急诊病人被迫转移。在我国，部分校园网用户受害严重，实验室数据和毕业设计被锁定加密，部分大型企业由于应用系统和数据库文件被加密后无法正常工作。

感染 WannaCry 勒索病毒的计算机，其文件将会被加密锁死，黑客通常通过这种办法向受害者索要赎金，在受害者支付赎金之后再为其提供解密密钥恢复文件。但由于 WannaCry 勒索病毒会让黑客无法判断究竟哪些受害者支付了赎金，因此很难向支付赎金的受害者提供解密密钥，所以即便支付了赎金，受到 WannaCry 勒索病毒攻击的受害者也极有可能永久失去其文件。

WannaCry 勒索病毒可以分为蠕虫部分和勒索病毒部分。蠕虫部分用于传播并释放勒索病毒。勒索病毒部分用于加密用户文件并索要赎金。通过对 WannaCry 勒索病毒的分析，发现它先加密用户文件，在生成加密文件之后再删除原始文件，虽然有通过文件恢复类工具恢复原始未加密文件的可能，但是因为 WannaCry 勒索病毒对文件系统的修改操作太过频繁，致使被删除的原始文件数据块被覆盖，导致实际恢复效果极为有限。因此，在受 WannaCry

勒索病毒感染后，不应该支付赎金，可以使用一些安全厂商提供的解密工具而实质上是文件恢复工具尝试恢复一些被删除的文件，但由于其作用十分有限，所以在感染 WannaCry 勒索病毒之后只能做好丢失文件的准备，重装系统。

也正是由于在感染 WannaCry 勒索病毒之后几乎没有办法找回丢失的文件，因此，做好病毒预防工作极为重要，以下是几点预防措施。

（1）用户在开机时需断开网络，这样基本可以避免被勒索病毒感染。开机后应尽快想办法打上安全补丁，打好安全补丁后才能够联网。

（2）定期对计算机中的重要文件资料进行备份，养成定期备份的好习惯，这样，即便不小心中了病毒，丢失了文件，我们依旧有备份的文件避免自身的损失。

（3）定期对操作系统和计算机软件进行更新，不要将系统和软件的自动更新关闭，以保持系统和软件在漏洞方面的修复。

2）“熊猫烧香”病毒

用户被感染“熊猫烧香”病毒之后，一定大小的可执行文件图标就会全部改成“一只熊猫手捧三支香”的新图标。这一病毒能中止大量反病毒软件和防火墙软件进程，并可以通过网页浏览、局域网共享及 U 盘等多种途径快速传播。中毒的计算机即使重新安装了操作系统，如果不把系统盘以外的病毒删除干净，也很容易再次中毒，而且“熊猫烧香”还会破坏用户的系统 Ghost 备份，删除以 gho 为后缀的镜像文件，使得用户难以快速恢复系统。除了对本机的破坏，“熊猫烧香”还会不断地下载其他木马与病毒，并且盗取用户的各种网络账号，以达到牟利的目的。

“熊猫烧香”病毒自 2006 年 12 月初开始暴发，危害最烈之时，甚至国内多家门户网站都被种植这一病毒，个人用户感染者数量已经高达几百万。这一病毒还在互联网上引起恐慌，网民在各论坛上跟帖发表评论 545 万余条。

“熊猫烧香”这类病毒会感染系统盘以外的分区，包括移动硬盘和 U 盘等驱动器，在这些驱动器的根目录下生成 autorun 运行项目。当用户双击染毒的盘符时，就会让健康的系统感染上病毒。用户在使用外来的 U 盘和移动存储器时，按住 Shift 键后再接入系统，防止驱动器自动运行，并且用右键菜单中的“打开”查看存储器中的内容。如果发现驱动器的右键菜单上有 auto 或是自动播放的项目，则该驱动器有很大可能已经感染了病毒。曾经中过病毒的计算机的非系统分区也要注意，在清除病毒或重装系统后最好清理、检查可执行文件，以免运行被感染的可执行文件后再次中毒。

由于“熊猫烧香”及其变种会感染可执行文件和删除 Ghost 的备份文件，因此用户也应该事先防范。软件的安装程序使用 WinRAR 等压缩软件压缩存放，将做好的 Ghost 备份文件的 gho 后缀改名。用户建立的各种文档应该做多个备份，系统中“我的文档”的位置也最好定位在 C 盘以外的驱动器上。

由于“熊猫烧香”病毒以及各种变种感染系统后会屏蔽掉知名杀毒软件的进程，即使想在系统中安装杀毒软件，也会以失败而告终。更有甚者，一些变种会屏蔽用户的搜索关键字，当用户试图在网络上搜索一些和病毒相关的字眼时，浏览器会被强行关闭。所以，中了病毒的计算机往往很难自救，用户最好的选择是在备份相关文件后重装操作系统。

如果一时不方便重装操作系统，还可以采用如下方法暂时恢复系统使用。

（1）在计算机自检完毕进入操作系统前按键盘上的 F8 键，选择安全方式进入操作系统。

（2）进入系统后，运行 msconfig 命令启动“系统配置实用程序”，将“启动”标签中的不明程序禁用（如果不能判断，推荐全部禁用），再将“服务”项目中的非微软服务全部禁用。

（3）运行 CMD 命令进入命令行方式。依次在所有硬盘分区根目录下输入 attrib - h*.* 命令，然后用 del autorun.inf 删除病毒的自动运行项目。

经过以上三步处理后，能暂时清除“熊猫烧香”和一些变种，使系统恢复可用状态。当然，最好的办法还是重装系统后彻底清除染毒可执行文件和各个驱动器的自动运行程序。

为了更好地防御此类病毒，对于大多数的用户来说，安装一款合适的防病毒软件是非常必要的。国内的 360、瑞星、江民、金山毒霸或是国外的诺顿、卡巴斯基等都有很好的查杀毒能力。其次，及时打好 Windows 的修正程序。目前个人计算机和商务计算机上安装使用的都是美国微软公司的 Windows 系列操作系统。Windows 系统推出后，微软公司经常发布修正系统 bug 的修正程序。用户最好使用 Windows 系统的更新功能自动下载修正程序，修正系统的 bug，提高系统的稳定性和安全性，因为很多病毒的传播和破坏都是利用了 Windows 的 bug。及时修正这些 bug，使得病毒无“后门”可进。

3）飞客蠕虫病毒

飞客蠕虫最早发现于 2008 年 11 月，它以 Windows 操作系统为攻击目标，现存在 A、B、B++、C、E 5 个主要变种，这些变种的功能和隐蔽性比原始程序更强。

飞客蠕虫病毒主要是借助闪存、利用微软的 MS08-067 漏洞以及通过加挂自带的字典猜解存在弱口令主机使用 IPC$通道进行传播的。当飞客病毒进入系统后，首先破坏系统中的默认属性设置，接着会自动扫描局域网内其他计算机是否存在 MS08-067 漏洞或者弱口令，一旦发现有问题的计算机系统，就会通过漏洞攻击或者通过 IPC$通道进行远程感染。如果受感染的计算机插入 U 盘，飞客蠕虫就会向 U 盘写入病毒体，创建 Autorun.inf，当其他计算机插入此 U 盘，即可通过“自动运行”的功能受到感染。

飞客蠕虫的病毒主体仅仅是一个动态链接库（DLL）文件，不同于传统的一些蠕虫病毒。传统病毒主体往往是一个可执行的.exe 文件。这些蠕虫病毒可能是自身就带有病毒功能，也可能是运行后释放出带有病毒功能的 DLL 或者 sys 文件。飞客蠕虫只有一个 DLL 文件，这种蠕虫主体文件本身无法直接执行，但是可以用 rund1132.exe 加载或者作为模块加载在其他进程中运行。同时，与以往病毒相比，飞客蠕虫可以通过 P2P 自我更新，这也就意味着通过它，控制者可以随时为其升级，实现各种功能。飞客蠕虫在系统中运行之后，首先会检查 Workstation、Server 和 Computer browser 这 3 个服务，如果有其中一个服务未启动，则病毒功能终止。如果这 3 个服务都启动，则蠕虫启动相应的病毒功能，枚举局域网内的 IP 地址，并对每个存活的主机尝试进行 MS 08-067 漏洞利用攻击，一旦攻击成功，就会将自身复制到被攻陷的系统中，并在其内存中运行。

首先，在受害主机 IH 上通过 ping 命令和浏览百度等网站证明网络是畅通的，可以正常上网。然后，试图访问微软公司的恶意软件删除工具网站，结果发现不能访问，这是显著的飞客蠕虫中毒现象，即不能访问许多系统升级和病毒软件升级网站。

确定主机 IH 是被蠕虫病毒感染后，接下来的任务就是要找出具体感染病毒的文件，准确报出病毒名称，并对其进行查杀、清除等工作。

检测与清除步骤一：使用 Windows 恶意软件删除工具检测。通过主机 SPH 从互联网上下载 Microsoft 的 Windows 恶意软件删除工具 Windows-KB890830-V4.13.exe，在主机 IH 上进行病毒检测。

检测与清除步骤二：使用 Windows 清理助手进行检测。通过主机 SPH 从互联网上下载 Windows 清理助手 arswp3_ x86.zip，在主机 IH 上进行病毒检测。结果发现该工具检测到 8 个可清理对象，并导出这 8 个可清理对象的文件备份到“病毒检测结果文件.zip”，以待验证。

检测与清除步骤三：使用 Windows 清理助手进行病毒清除。在检测结果界面图选中全部对象，然后单击“执行清理”按钮就可以清除病毒。

12. 分析蠕虫与病毒的区别，收集资料，解析下面蠕虫的关键技术。

（1）蠕虫王。

（2）震荡波。

答：病毒和蠕虫都会导致计算机信息遭到破坏，它们可能使你的网络和操作系统变慢，危害严重时甚至会完全破坏系统，并且，它们还可能使用你的计算机将它们自己传播给你的朋友、家人、同事以及 Web 的其他地方，在更大范围内造成危害。他们都是人为编制出的恶意代码，都会对用户造成危害，人们往往将它们统称为病毒，但其实这种称法并不准确，它们之间虽然有共性，但也有很大的差别。

计算机病毒（computer virus）根据《中华人民共和国计算机信息系统安全保护条例》，病毒的明确定义是指“编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。病毒必须满足两个条件：它必须能自行执行；它必须能自我复制。蠕虫（worm）也可以算是病毒中的一种，但是它与普通病毒之间有很大的区别。一般认为，蠕虫是一种通过网络传播的恶性病毒，它具有病毒的一些共性，如传播性、隐蔽性、破坏性等，同时具有自己的一些特征，如不利用文件寄生(有的只存在于内存中)，对网络造成拒绝服务，与黑客技术相结合，等等。普通病毒需要传播受感染的驻留文件进行复制，而蠕虫不使用驻留文件即可在系统之间进行自我复制，普通病毒的传染能力主要是针对计算机内的文件系统而言，而蠕虫病毒的传染目标是互联网内的所有计算机。它能控制计算机上可以传输文件或信息的功能，一旦系统感染了蠕虫，蠕虫即可自行传播，将自己从一台计算机复制到另一台计算机，更危险的是，它还可大量复制。因而，在产生的破坏性上，蠕虫病毒也不是普通病毒能比拟的，网络的发展使得蠕虫可以在短短的时间内蔓延整个网络，造成网络瘫痪!

（1）蠕虫王：该蠕虫攻击安装有 Microsoft SQL 的 NT 系列服务器，该病毒尝试探测被攻击机器的 1434/UDP 端口，如果探测成功，则发送 376B 的蠕虫代码 1434/UDP 端口为 Microsoft SQL 开放端口。该端口在未打补丁的 SQL Server 平台上存在缓冲区溢出漏洞，使蠕虫的后续代码能够有机会在被攻击机器上运行进一步传播，导致系统瘫痪，停止服务。攻击对象多为 Windows XP、Windows NT，不攻击 Windows 9X。

（2）震荡波：具体技术特征如下。

A. 感染系统为 Windows 2000、Windows Server 2003、Windows XP、Windows 7。

B. 利用微软的漏洞 MS04-011。

C. 病毒运行后，会自身复制为%WinDir%\napatch.exe。

D. 在注册表启动项 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Run 下创建："napatch.exe" = %WinDir%\napatch.exe；这样，病毒在 Windows 启动时就得以运行。

E. 在 TCP 端口 5554 建立 FTP 服务，用以自身传播给其他计算机。

F. 随机在网络上搜索机器，向远程计算机的 445 端口发送包含后门程序的非法数据，远程计算机如果存在 MS04-011 漏洞，就会自动运行后门程序，打开后门端口 9996。病毒利用后门端口 9996，使得远程计算机连接病毒打开的 FTP 端口 5554，下载病毒体并运行，从而遭到感染。

G. 病毒还会利用漏洞攻击 lsass.exe 进程，被攻击计算机的 lsass.exe 进程会瘫痪，Windows 系统会有 1 分钟倒计时关闭的提示。

H. 病毒在 C:\win32.log 中记录其感染的计算机数目和 IP 地址。

13. 收集资料，讨论针对当前 3 种流行木马的防范及清除策略。

答：（1）“网络公牛”。

此种流行木马程序没有采用文件关联功能，采用的是文件捆绑功能，要清除其非常困难！你可能要问：那么其他木马为什么不用这个功能？防范要点是监测易被捆绑文件长度，如果发现文件长度发生了变化，就可初步断定自己中了“网络公牛”木马病毒。

清除方法：

A. 删除网络公牛的自启动程序 C:\WINDOWS\SYSTEM\CheckDll.exe。

B. 把网络公牛在注册表中建立的键值全部删除（上面列出的那些键值全部删除）。

C. 检查上面列出的文件，如果发现文件长度发生变化（大约增加了 40KB，可以通过与其他机子上的正常文件比较而知），就删除它们！然后单击“开始→附件→系统工具→系统信息→工具→系统文件检查器”，在弹出的对话框中选中“从安装软盘提取一个文件(E)”，在框中填入要提取的文件（前面你删除的文件），单击“确定”按钮，然后按屏幕提示将这些文件恢复即可。如果是开机时自动运行的第三方软件，如 realplay.exe、QQ、ICQ 等被捆绑上了，那就得把这些文件删除，再重新安装。

（2）网络神偷。

网络神偷又名 Nethief，是第一个反弹端口型木马。大多数的防火墙对于由外面连入本机的连接都会进行非常严格的过滤，但是对于由本机发出的连接，却疏于防范（当然，有的防火墙两方面都很严格）。于是，与一般的木马相反，反弹端口型木马的服务端（被控制端）使用主动端口，客户端（控制端）使用被动端口，当要建立连接时，由客户端通过 FTP 主页空间告诉服务端：“现在开始连接我吧！”并进入监听状态，服务端收到通知后，就会开始连接客户端。为了隐蔽起见，客户端的监听端口一般开在 80，这样，即使用户使用端口扫描软件检查自己的端口，发现的也是类似“TCP 服务端的 IP 地址：1026 客户端的 IP

地址：80 ESTABLISHED”的情况，稍微疏忽一点就会以为是自己在浏览网页。因为没有哪个防火墙不给用户向外连接 80 端口。

清除方法：

A. 网络神偷会在注册表 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下建立键值 internet，其值为 internet.exe /s，将键值删除。

B. 删除其自启动程序 C:\WINDOWS\SYSTEM\INTERNET.EXE。

（3）WAY2.4。

WAY2.4 又称火凤凰、无赖小子，是国产木马程序，默认连接的端口是 8011。众多木马高手在介绍这个木马时都对其强大的注册表操控功能赞不绝口，也正因为如此，它对我们的威胁就更大了。WAY2.4 的注册表操作的确有特色，对受控端注册表的读写，就和对本地注册表的读写一样方便。

WAY2.4 服务端被运行后在 C:\windows\system 下生成 msgsvc.exe 文件，图标是文本文件的图标，很隐蔽，文件大小为 235008B，文件修改时间为 1998 年 5 月 30 日，看来它想冒充系统文件 msgsvc32.exe。同时，WAY2.4 在注册表 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下建立串值 Msgtask，其键值为 C:\WINDOWS\SYSTEM\msgsvc.exe。此时如果用进程管理工具查看，会发现进程 C:\windows\system\msgsvc.exe 赫然在列！

清除方法：

要清除 WAY，只要删除它在注册表中的键值，再删除 C:\windows\system 下的 msgsvc.exe 文件就可以了。注意，在 Windows 下直接删除 msgsvc.exe 是删不掉的，此时可以用进程管理工具终止它的进程，然后再删除它。或者到 DOS 下删除 msgsvc.exe。如果服务端已经与可执行文件捆绑在一起了，那就只有将那个可执行文件也删除了！删除前请做好备份。

14. 什么叫网络木马攻击？

答：网络木马攻击是指系统中被植入的、人为设计的程序，目的包括通过网络远程控制其他用户的计算机系统，窃取信息资料，并恶意致使计算机系统瘫痪等。

RFC（Request for Comments，IETF 制定的 Internet 标准草案）1244 中是这样描述网络木马攻击的：“木马程序是一种程序，它能提供一些有用的，或是仅令人感兴趣的功能。但是，它还有用户不知道的其他功能，例如，在你不了解的情况下复制文件或窃取你的密码。”这个定义虽然不十分完善，但是可以澄清一些模糊的概念。首先，木马程序并不一定实现某种对用户来说有意义或有帮助的功能，但却会实现一些隐藏的、危险的功能；其次，木马实现的主要功能并不为受害者所知，只有木马程序编制者最清楚；第三，这个定义暗示“有效负载”是恶意的。

一个完整的木马套装程序含两部分：服务端（服务器部分）和客户端（控制器部分）。植入对方计算机的是服务端，而黑客正是利用客户端进入运行了服务端的计算机。运行了木马程序的服务端以后，会产生一个容易迷惑用户的名称的进程，暗中打开端口，向指定地点发送数据（如网络游戏的密码、实时通信软件密码和用户上网密码等），黑客甚至可以利用这些打开的端口进入计算机系统。这时你计算机上的各种文件、程序，以及在你计算

机上使用的账号、密码就无安全可言了。

15. 木马有哪些危害？

答：木马程序具有很大的危害性，主要表现在：自动搜索已中木马的计算机；管理对方资源，如复制文件、删除文件、查看文件内容、上传文件、下载文件等；跟踪监视对方屏幕；直接控制对方的键盘、鼠标；随意修改注册表和系统文件；共享被控计算机的硬盘资源；监视对方运行的任务且可终止对方任务；远程监测和操纵计算机。

16. 木马按破坏功能分为哪几种？

答：（1）破坏型。

（2）密码发送型。

（3）远程访问型。

（4）键盘记录木马。

（5）DoS 攻击木马。

（6）代理木马。

（7）FTP 木马。

（8）程序杀手木马。

（9）反弹端口型木马。

17. 典型木马有哪些特性和辅助特点？

答：木马的特性包括有效性、隐蔽性、顽固性和易植入性。

辅助特点是自动运行、欺骗性、自动恢复和功能的特殊性。

18. 木马有哪些植入技术？

答：木马植入技术可以分为主动植入与被动植入两类。

所谓主动植入，就是攻击者主动将木马程序种到本地或者远程主机上，这个行为过程完全由攻击者主动掌握。

而被动植入，是指攻击者预先设置某种环境，然后被动等待目标系统用户的某种可能的操作，只有这种操作执行，木马程序才可能植入目标系统。

19. 木马自动加载方式有哪几种？

答：在 Windows 系统中，木马程序的自动加载技术主要有：修改系统文件；修改系统注册表；添加系统服务；修改文件打开关联属性；修改任务计划；修改组策略；利用系统自动运行的程序；修改启动文件夹；替换系统 DLL 等。

20. 木马是如何隐藏自己的？

答：要隐藏木马的服务端，可采用伪隐藏或真隐藏。伪隐藏是指程序的进程仍然存在，只不过是让它消失在进程列表里。真隐藏则是让程序彻底消失，不以一个进程或者服务的方式工作。

21. 请举例说明几种常见的木马程序和使用端口号。

答：木马程序和使用端口号列表见表 1-1。

表 1-1　木马程序和使用端口号列表

端口号	木马软件	端口号	木马软件
8102	网络神偷	23445	网络公牛（netbull）
2000	黑洞 2000	31338	Back Orifice、DeepBO
2001	黑洞 2001	19191	蓝色火焰
6267	广外女生	31339	Netspy Dk
7306	网络精灵 3.0（Netspy 3.0）	40412	The Spy
7626	冰河	1033	Netspy
8011	WRY、赖小子、火凤凰	121	BO jammerkillahv
23444	网络公牛（Netbull）	4590	ICOTrpjan

22. 木马的远程监控功能有哪些？

答：木马的远程监控功能概括起来有以下几点：获取目标机器信息、记录用户事件、远程操作。

23. 如何对木马进行防御？

答：对木马进行防御可以采用端口扫描和连接检查，检查系统进程，检查 ini 文件、注册表和服务，监视网络通信等方法。

24. 简述常见的黑客攻击过程。

答：常见的黑客攻击过程如图 1-1 所示。

25. 比较病毒、蠕虫、木马、后门和僵尸。

答：病毒、蠕虫、木马、后门和僵尸比较见表 1-2。

表 1-2　病毒、蠕虫、木马、后门和僵尸比较

类型	存在形式	自我复制	传播方式	运行方式	攻击后果
病毒	寄生	有	文件感染	自主，可触发	文件感染
蠕虫	独立	有	网络	自主	消耗资源
木马	隐蔽独立	无	被植入	受控	窃取信息
后门	寄生	无	被植入	受控	帮助攻击
僵尸	寄生	无	被植入，网络	自主	发动分布式拒绝服务攻击

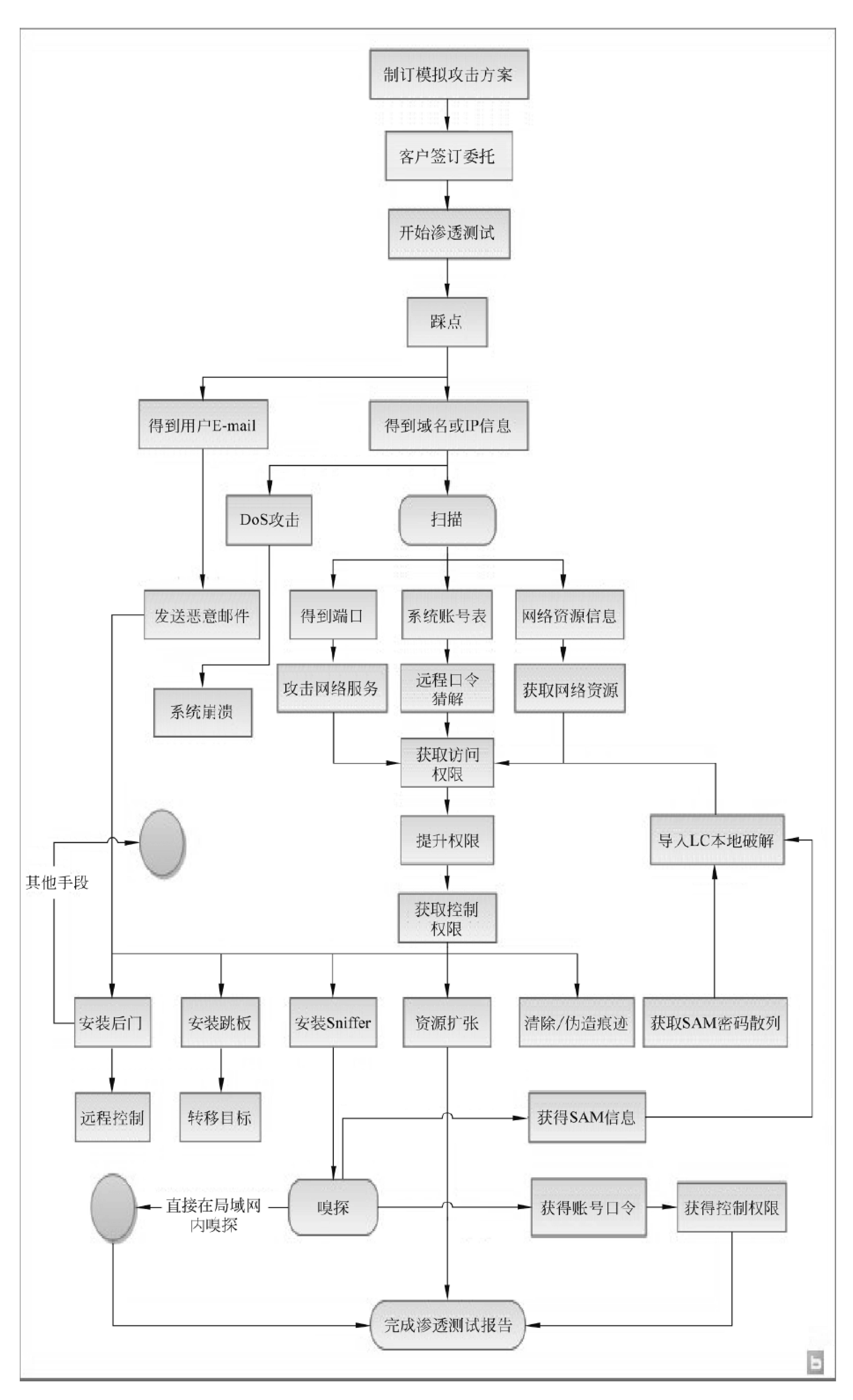


图 1-1　常见的黑客攻击过程

26. 收集国内外有关病毒和其他恶意程序的网站信息，简要说明各网站的特点。

答：犯罪分子常利用顶级域名的模糊改变欺骗用户。顶级域名是网络的重要组成部分，一个网站的最后几个字母代码能告诉我们它是在哪里注册的。也许每个人都认识.com 和 .gov，但还有很多顶级域名（TLD）对许多人来说可能很陌生。例如，.am 代表亚美尼亚，.cm 代表喀麦隆。骗子就是从用户的无知中获利的，许多消费者在搜索时从来不注意顶级域名的后缀。许多消费者都会单击第一个看上去有意思的结果，而犯罪分子有足够的时间为搜索引擎优化自己的网站，这样消费者就掉入了骗子们的圈套。

犯罪分子是如何滥用顶级域名进行非法交易的？举例来说，网站很有可能植入一个流氓反病毒程序，希望消费者认为这是一个警告："你计算机中有病毒，请安装此软件。"这种注册商辛苦防范的行为被称为"误植域名"。误植域名涉及各种各样的网站：如从用户输入错误中获得广告收入的网站，向你推销会窃取个人信息或安装恶意软件的成熟的钓鱼网站地址的网站等。

五大风险注册比例最高的顶级域名分别是：.com（商业广告），.info（信息），.vn（越南），.cm（喀麦隆），.am（亚美尼亚）。

全球分布在前 20 个最危险的顶级域名中，有 7 个来自欧洲、中东和非洲地区，包括新进入前 20 榜单的亚美尼亚（.am）和波兰（.pl）。亚太地区以 6 个危险顶级域名位列第二，而通用域名，如 Network（.net）占了前 20 中的 5 席。唯一进入前 20 的美国域名是 United States（.us）。

27. 总结各种电磁波窃听方法的技术要点，提出相应的防范设想。

答：电磁波窃听可以截获信息，它有两种技术，即信号拦截窃听和电磁泄露窃听。信号拦截窃听也称为搭线窃听。例如，将窃听器的两根接线接到电话线路上，直接截获电话线路中的电流信号。另外，还可以根据电磁感应现象将感应线圈设置在电话线外，电话机下，窃听通话内容。而电磁泄露窃听是指利用电子设备中的杂散能量的扩散捕获电磁泄露信号。可以在距离更远的地方捕获强度更弱的电磁波信号。

对于电磁波窃听的防范，有以下措施：①屏蔽；②隔离；③低辐射；④使用干扰器；⑤滤波；⑥接地；⑦数据加密和数据隐藏。

28. 收集各种手机监听技术要点，提出相应的防范设想。

答：手机监听主要有三种技术，具体介绍如下。

（1）截获手机电磁波，如设立伪基站系统，相隔数万里的人们能够通过手机对话，靠的就是附近的基站。一方面，基站接收信号；另一方面，基站负责将信号传递出去，在通话者之间充当着"桥梁"的作用。而这个伪基站并不传输信号，只接收信号。伪基站大小不一，规模小点的伪基站和计算机主机差不多，但是它却能接收到周围所有的通信信号。虽然接收那么多信号，但这个阻截器可以聪明地辨别，找到打算窃听的那个手机。奥秘就在于伪基站能在空中获取每部手机的 IMSI 号。IMSI 号就像手机的"身份证号"，独一无二。伪基站获取这个号码后，这个手机上发出的所有信号都被拦截。防范方法包括提高对不明短信和不明号码的鉴别能力以及采用手机反窃听设备。

（2）安装手机卧底软件——木马程序。

防范手段有：首先，要从正规渠道购买手机。其次，不要随便到非指定维修点修理手机，不要轻易将手机借给别人使用，另外可以定期刷新手机系统。

（3）复制 SIM 卡。

如果 SIM 卡被复制，手机隐私将会泄露。在有母卡的情况下，复制 SIM 卡是一件很容易的事情，不过，在没有母卡的情况下，复制 SIM 卡的难度相当大。防窃听方法：遗失 SIM 卡后尽早挂失，一般情况下，要防止 SIM 卡被复制，手机用户须保管好自己的手机 SIM 卡以及密码，不法分子就不可能凭空克隆手机卡。用户一旦丢失 SIM 卡，应该立刻挂失。

29. 收集各种网络监听技术要点，提出相应的防范设想。

答：这里主要讨论局域网中以太网络的监听技术（或称嗅探技术）。以太网有两种形式：共享式和交换式。在共享式局域网中，如果将某一台主机的网卡设置成混杂模式，那么，对这台主机的网络接口而言，在这个局域网内传输的任何信息都是可以被听到的，主机的这种状态也就是监听模式。处于监听模式下的主机可以嗅探到同一个网段下的其他主机发送信息的数据包。网卡接收到数据包后，就会将其传给上一层处理，如果在这一阶段使用嗅探软件提供一定的捕获和过滤机制，就可以达到监听信息的目的。

交换式以太网是用交换机或其他非广播式交换设备组建成的局域网。这些设备根据收到的数据帧中的 MAC 地址决定数据帧应发向交换机的哪个端口。由于端口间的帧传输彼此屏蔽，在很大程度上解决了网络嗅探的困扰，但随着嗅探技术的发展，交换式以太网中同时存在网络嗅探的安全隐患。黑客可以通过溢出攻击和 ARP 欺骗技术迫使交换机退回到广播模式实现监听。这就是和交换式局域网与共享式局域网的监听区别，对于交换式局域网，实施监听首先要进行溢出攻击或 ARP 欺骗。

虽然共享式局域网中的嗅探很隐蔽，但也有一些方法帮助判断：检测处于混杂模式的网卡，网络通信丢包率非常高，网络带宽出现反常检测技术，网络与主机响应时间测试和 ARP 检测（如 ANTI SNIFF 工具）等。

在交换网络下防监听，主要是防御 ARP 欺骗及 ARP 过载。防御 ARP 欺骗的措施主要包括：不要把网络安全信任关系建立在单一的 IP 或 MAC 基础上，理想的关系应该建立在 IP-MAC 对应关系的基础上。

使用静态的 ARP 或者 IP-MAC 对应表代替动态的 ARP 或者 IP-MAC 对应表，禁止自动更新，使用手动更新。定期检查 ARP 请求，使用 ARP 监视工具，如 ARPWatch 等监视并探测 ARP 欺骗，制定良好的安全管理策略，加强用户安全意识。

ARP 过载则是指通过发送大量 ARP 数据包，使得交换设备出现信息过载，被迫工作于广播模式。这时系统管理人员可以通过在本地网络中加入交换设备，预防 ARP 过载导致监听嗅探的侵入。

30. 收集资料，比较下列传输介质上信息被监听的机会和可能。

（1）以太网。

（2）令牌网。

（3）电话网。

（4）有线电视网。

（5）微波和无线电。

答：（1）以太网：因为以太网是一种广播型网络，所以大多数网络数据的截获是在这种网络上实现的，被监听的机会和可能很大。

（2）令牌网：尽管令牌网并不是一个广播型网络，但带有令牌的那些包在传输过程中，平均要经过网络上一半的计算机，使得网络监听成为可能，但是令牌网中高的数据传输率使网络监听实现起来变得非常困难。

（3）电话网：有线电话网可以被一些电话公司协作人或者一些有机会在物理上访问到线路的人搭线窃听。无线电话网被监听的可能性较大。

（4）有线电视网：对于智能电视网，存在监听的可能性很大。普通有线电视网除非是相关管理人员进行的监听，其他情况下被监听的概率小。

（5）微波和无线电：监听的可能性高。无线电本来就是一个广播性的传输媒介，任何一个无线电接收机都可以截获传输的信息。在微波线路上的信息也会被截获。在实际中，高速的调制解调器将比低速的调制解调器搭线窃听困难一些，因为高速调制解调器中引入了许多频率。CDMA 比 GSM 监听的可能性小一些。

31. 请解释以下 5 种“窃取机密攻击”方式的含义。

（1）网络踩点（footprinting）。

（2）扫描攻击（scanning）。

（3）协议栈指纹（stack fingerprinting）鉴别（也称操作系统探测）。

（4）信息流嗅探（sniffering）。

（5）会话劫持（session hijacking）。

答：（1）在典型的入侵过程中，攻击者在实际攻击前会先进行信息收集和分析工作，也就是所谓的“网络踩点”。Web 页面盗窃同样也是为了完成 Web 攻击前的踩点工作，试图寻找 Web 应用和服务器中可能存在的安全漏洞。攻击者通过对各个网页页面源码的详细分析，找出可能存在于代码、注释或者设计中的缺陷和脆弱点，以此确定攻击的突破口。

（2）扫描攻击是一种自动检测远程或本地主机安全性弱点的程序。它集成了常用的各种扫描技术，能自动发送数据包去探测和攻击远端或本地的端口和服务，并自动收集和记录目标主机的反馈信息，从而发现目标主机是否存活、目标网络内使用的设备类型与软件版本、服务器或主机上各 TCP/UDP 端口的分配、所开放的服务、所存在的可能被利用的安全漏洞，据此提供一份可靠的安全性分析报告，报告信息系统可能存在的脆弱性。

（3）利用 TCP/IP 堆栈作为特殊的“指纹”，以确定操作系统类型的技术称为协议栈指纹识别。识别操作系统（Operating System，OS）类型是入侵或分析漏洞和各种安全隐患的基础，可分为主动协议栈指纹识别和被动协议栈指纹识别。例如，FIN 探测主动协议栈指纹识别通过向目标主机上的一个打开的端口发送一个 FIN 分组，然后等待回应；根据回应信息判断操作系统类型，而被动协议栈指纹识别从不主动发送数据包，只是被动地捕获远程主机返回的包分析其 OS 类型版本，如根据 TTL（Time To Live）值判断，TTL 值是操作系

统对出站的信息包设置的存活时间，不同操作系统设计的值不一样。

（4）信息流嗅探也可称为信息流监听，也就是在通话双方未授权的情况下实施非法窃听或嗅探。这里主要是指网络监听，可以分为共享式和交换式两种情况。共享式局域网中，如果将某一台主机的网卡设置成混杂模式，那么，对这台主机的网络接口而言，在这个局域网内传输的任何信息都是可以被听到的，主机的这种状态也就是监听模式。处于监听模式下的主机可以嗅探到同一个网段下的其他主机发送信息的数据包。网卡接收到数据包后，就会将其传给上一层处理，如果在这一阶段使用嗅探软件提供一定的捕获和过滤机制，就可以达到监听信息的目的。交换式以太网是用交换机或其他非广播式交换设备组建成的局域网。这些设备根据收到的数据帧中的 MAC 地址决定数据帧应发向交换机的哪个端口。端口间的帧传输彼此屏蔽，在很大程度上解决了网络嗅探的困扰，但随着嗅探技术的发展，交换式以太网中同时存在网络嗅探的安全隐患。黑客可以通过溢出攻击和 ARP 欺骗技术迫使交换机退回到广播模式实现监听。这就是和交换式局域网与共享式局域网的监听区别，对于交换式局域网，实施监听首先要进行溢出攻击或 ARP 欺骗。

（5）会话劫持结合了网络嗅探及 IP 欺骗技术。会话劫持成功后会在用户不知情下接管一个现存动态会话过程，即攻击者通过会话劫持可以替代原来的合法用户，同时能够监视并掌握会话内容。攻击者可以对受害者的回复进行记录，并在接下来的时间里对其进行响应，展开进一步的欺骗和攻击。会话劫持结合了网络嗅探及欺骗技术。

32. 请解释以下 5 种“非法访问”攻击方式的含义。

（1）口令破解。

（2）IP 欺骗。

（3）DNS 欺骗。

（4）重放（replay）攻击。

（5）特洛伊木马（trojan horse）。

答：（1）口令机制是资源访问的第一道屏障。攻破这道屏障，就获得了进入系统的第一道大门。口令的作用是向系统提供唯一标识个体身份的机制，只给个体所需信息的访问权，从而达到保护敏感信息和个人隐私的作用。而黑客利用口令破解达到窃取机要信息的目的。常用口令破解方法有词典破解、暴力破解或穷举法、组合攻击等。还有社会工程学、偷窥、搜索垃圾箱、口令蠕虫、特洛伊木马、网络监听、重放等其他方法。

（2）欺骗实质上就是一种冒充身份通过认证骗取信任的攻击方式。攻击者针对认证机制的缺陷，将自己伪装成可信任方，从而与受害者进行交流，最终攫取信息或是展开进一步攻击。IP 欺骗就是伪装成其他计算机的 IP 地址骗取连接，获得信息或者得到特权；最基本的 IP 欺骗技术有三种：简单的 IP 地址变化、源路由攻击和利用 UNIX 系统的信任关系。

（3）DNS 的全称是 Domain Name Server，即域名服务器。DNS 的功能是提供主机域名和 IP 地址之间的转换信息。DNS 欺骗就是利用域名与 IP 地址转换过程中实现的欺骗。

（4）重放攻击：又称重播攻击、回放攻击，是指攻击者发送一个目的主机已接收过的包，达到欺骗系统的目的，主要用于身份认证过程，破坏认证的正确性。重放攻击可以由发起者进行，也可以由拦截并重发该数据的敌方进行。攻击者利用网络监听或者其他方式

盗取认证凭据，之后再把它重新发给认证服务器。重放攻击在任何网络通信过程中都可能发生，是计算机世界黑客常用的攻击方式之一。

（5）特洛伊木马：特洛伊木马目前一般可理解为“为进行非法目的的计算机病毒”，在计算机中潜伏，以达到黑客目的。一个完整的特洛伊木马套装程序含了两部分：服务端（服务器部分）和客户端（控制器部分）。植入对方计算机的是服务端，而黑客正是利用客户端进入运行了服务端的计算机。运行了木马程序的服务端以后，会产生一个容易迷惑用户的名称的进程，暗中打开端口，向指定地点发送数据（如网络游戏的密码、实时通信软件密码和用户上网密码等），黑客甚至可以利用这些打开的端口进入计算机系统。这时你计算机上的各种文件、程序，以及在你计算机上使用的账号、密码就无安全可言了。

33. 分析路由欺骗的原理，并与 ARP 欺骗和 DNS 欺骗进行比较。

答：路由欺骗的原理如下：源路由机制通过 IP 数据包报头的源路由选项字段工作，它允许数据包的发送者在这一选项里设定接收方返回的数据包要经过的路由表，包括两种类型：

（1）宽松的源站选择（LSR）

发送端指明数据包必须经过的 IP 地址清单，但如果需要，也可以经过除这些地址以外的其他地址。

（2）严格的源站选择（SRS）

发送端指明数据包必须经过的确切地址。如果没有经过这一确切路径，数据包会被丢弃，并返回一个 ICMP 报文。换句话说，在传送过程中，必须考虑数据包经过的确切路径，如果由于某种原因没有经过这条路径，这个数据包就不能被发送。

源路由选项字段长 39B，除去其中 3B 的附加信息，剩下的 36B 仅对应 9 个 IP 地址空间，由于最后一个地址必须是目的地址，所以实际上只能填写 8 个 IP 地址。随着互联网的发展，路由经过的 IP 地址数通常都会大于 8 个，在这种情况下，使用宽松的源站选路比较妥当，因为如果不能找到确切的路径，严格的源路由选路就会丢弃这个数据包。

ARP 欺骗原理：主机在实现 ARP 缓存表的机制中存在一个不完善的地方，那就是主机收到一个 ARP 应答包后，它并不会去验证自己是否发送过对应的 ARP 请求，也不会验证这个 ARP 应答包是否可信，而是直接用应答包里的 MAC 地址与 IP 地址的对应关系替换掉 ARP 缓存表中原有的相应信息。ARP 欺骗攻击的实现正是利用了这一点。

DNS 欺骗：DNS 的全称是 Domain Name Server，即域名服务器，是一种用于 TCP/IP 应用程序的分布式数据库，它提供主机域名和 IP 地址之间的转换信息。当客户主机向本地 DNS 服务器查询域名的时候，如果服务器的缓存中已经有相应记录，DNS 服务器就不会再向其他服务器进行查询，而是直接将这条记录返回给用户。攻击者正是利用这一点，在 DNS 服务器的本地 Cache 中缓存一条伪造的解析记录实现 DNS 欺骗的。

这样看来，正如名称中所说的路由欺骗，ARP 欺骗和 DNS 欺骗是分别利用路由信息，ARP 缓存中 MAC 地址和 IP 地址的对应关系，以及 DNS 中主机域名和 IP 地址的对应关系的篡改达到欺骗的目的。

34. IP 欺骗有哪些方法？

答：最基本的 IP 欺骗技术有三种：简单的 IP 地址变化、源路由攻击、利用 UNIX 系统的信任关系。

35. 请描述局域网间通信时一次完整的 ARP 欺骗过程。

答：现在假设主机 A（192.168.1.2）要与主机 B（192.168.1.3）通信。A 首先会检查自己的 ARP 缓存中是否有 IP 地址 192.168.1.3 对应的 MAC 地址。如果有，则直接使用对应的 MAC 地址；如果没有，它就会在局域网内广播 ARP 请求包，内容是“192.168.1.3 的 MAC 地址是什么？请告诉 192.168.1.2”。

局域网内的所有主机都会收到这个请求包，但只有 IP 地址为 192.168.1.3 的这台主机才会响应，它会回应 192.168.1.2 一个 ARP 应答包，内容是“192.168.1.3 的 MAC 地址是 03-03-03-03-03-03”。

这样，主机 A 就得到了主机 B 的 MAC 地址，并且它会把这个对应的关系存在自己的 ARP 缓存表中。之后，主机 A 与主机 B 之间的通信就依靠两者缓存表里的 MAC 地址通信了，直到通信停止后两分钟，这个对应关系才会被从表中删除。

主机在实现 ARP 缓存表的机制中存在一个不完善的地方，那就是主机收到一个 ARP 应答包后，它并不会去验证自己是否发送过对应的 ARP 请求，也不会验证这个 ARP 应答包是否可信，而是直接用应答包里的 MAC 地址与 IP 地址的对应关系替换掉 ARP 缓存表中原有的相应信息。ARP 欺骗攻击的实现正是利用了这一点。

假设攻击者是主机 B（192.168.1.3），它向网关 C 发送一个 ARP 应答包宣称：“我是 192.168.1.2（主机 A 的 IP 地址），我的 MAC 地址是 03-03-03-03-03-03（攻击者的 MAC 地址）。同时，攻击者向主机 A 发送 ARP 应答包说：“我是 192.168.1.1（网关 C 的 IP 地址），我的 MAC 地址是 03-03-03-03-03-03（攻击者的 MAC 地址）。”

接下来，由于 A 的缓存表中 C 的 IP 地址已与攻击者的 MAC 地址建立了对应关系，所以 A 发给 C 的数据就会被发送到攻击者的主机 B，同时，C 发给 A 的数据也会被发送到 B。攻击者 B 就成了 A 与 C 之间的“中间人”，可以按其目的随意进行破坏了。

ARP 欺骗的一般过程如图 1-2 所示。

ARP 欺骗攻击在局域网内非常奏效，它可以导致同网段的其他用户无法正常上网（频繁断网或者网速慢），可以嗅探到交换式局域网内的所有数据包，从而获取敏感信息。此外，攻击者还可以在这一攻击过程中对信息进行篡改，修改重要的信息，进而控制受害者的会话。

36. 请描述一次完整的 DNS 欺骗过程。

答：DNS 的全称是 Domain Name Server，即域名服务器，是一种用于 TCP/IP 应用程序的分布式数据库，它提供主机域名和 IP 地址之间的转换信息。通常，网络用户通过 UDP 和 DNS 服务器进行通信，而服务器在特定的 53 端口监听，并返回用户所需的相关信息，这是“正向域名解析”的过程。“反向域名解析”也是一个查询 DNS 的过程，当客户向一台服务器请求服务时，服务器方根据客户的 IP 地址反向解析出该 IP 对应的域名。

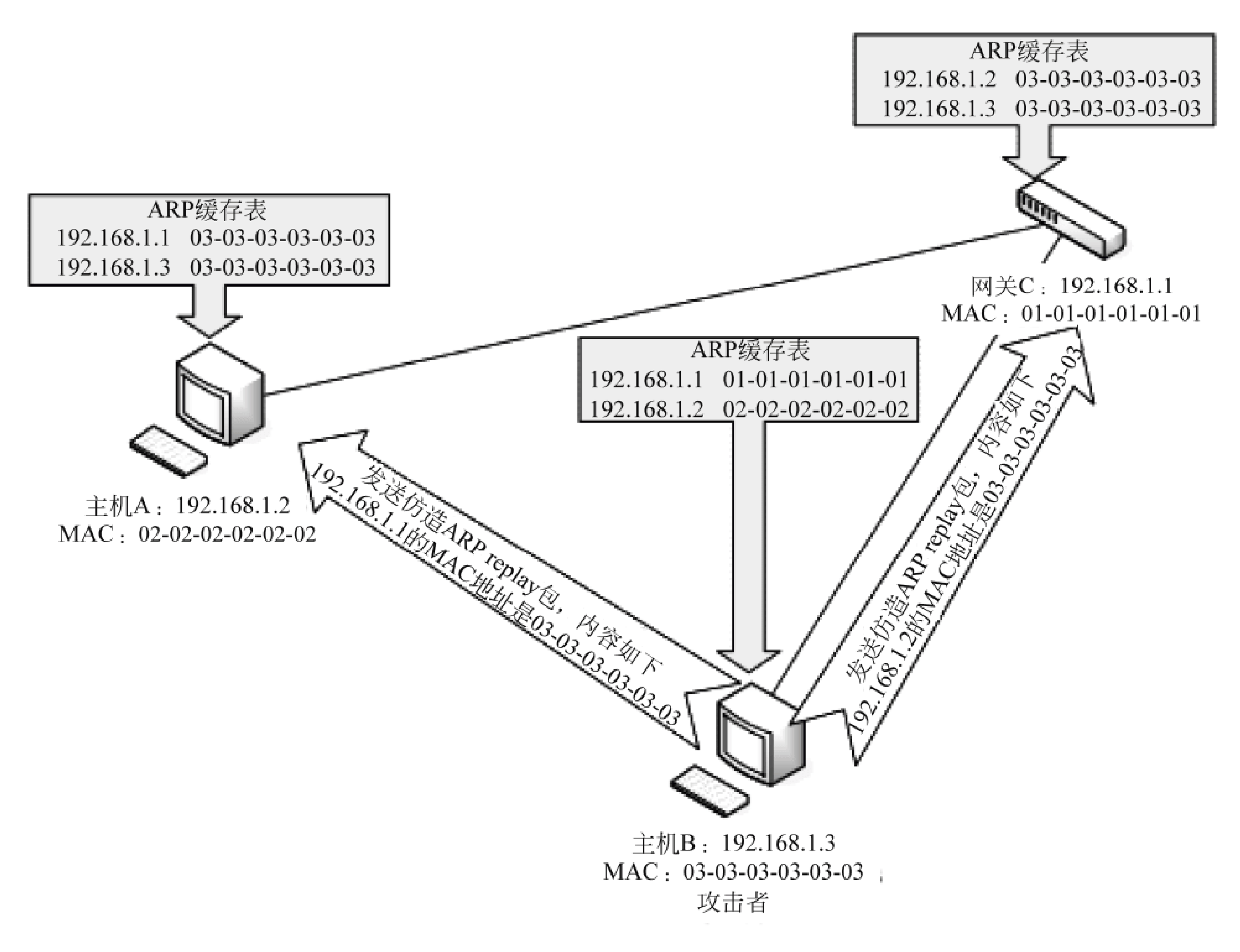


图 1-2　ARP 欺骗的一般过程

当客户主机向本地 DNS 服务器查询域名的时候，如果服务器的缓存中已经有相应记录，DNS 服务器就不会再向其他服务器进行查询，而是直接将这条记录返回给用户。攻击者正是利用这一点，在 DNS 服务器的本地 Cache 中缓存一条伪造的解析记录实现 DNS 欺骗的。

攻击者怎样伪造 DNS 应答信息就成了问题的焦点。

一种可能是，攻击者控制了某个域名服务器（如 nipc.com 域），在其数据库中增加一个附加记录，将攻击目标的域名（如 www.dhs.com）指向攻击者的欺骗 IP。用户向该域名服务器发送对攻击目标的域名解析请求时，将得到攻击者的欺骗 IP，同时，域名服务器之间的通信也将使这一虚假的映射记录传播到其他域名服务器上，从而造成更多的用户受到欺骗。

不过，在现实情况中，攻击者往往无法控制 DNS 服务器，通常可以做到的是控制该服务器所在网络的某台主机，并可以监听该网络中的通信情况。这时，攻击者要对远程的某个 DNS 服务器进行欺骗攻击，采用的手段很像 IP 欺骗攻击。首先，攻击者要冒充某个域名服务器的 IP 地址；其次，攻击者要能预测目标域名服务器发送的 DNS 数据包的 ID 号。

DNS 数据是通过 UDP 传递的，在 DNS 服务器之间进行域名解析通信时，请求方和应答方都使用 UDP 53 端口，而这样的通信过程往往是并行的。也就是说，DNS 域名服务器之间同时可能会进行多个解析过程，既然不同的过程使用的是相同的端口号，那靠什么区别它们呢？答案在 DNS 报文里面。

在 DNS 报文格式头部的 ID 域是用来匹配响应和请求数据报文的。只有使用相同的 ID 号，才能证明是同一个会话（由请求方决定所使用的 ID）。不同的解析会话采用不同的 ID

号。在域名解析的整个过程中，请求方首先以特定的标识（ID）向应答方发送域名查询数据包，而应答方以相同的 ID 号向请求方发送域名响应数据包，请求方会将收到的域名响应数据包的 ID 和自己发送的查询数据包的 ID 相比较，如果相同，则表明接收到的正是自己等待的数据包，如果不相同，则丢弃。

如果攻击者伪造的 DNS 应答包中含有正确的 ID 号，并且抢在 dhs.com 域的 DNS 服务器之前向 nipc.com 域的 DNS 服务器返回伪造信息，欺骗攻击就将获得成功。于是，确定目标 DNS 服务器的 ID 号即为 DNS 欺骗攻击的关键所在。在一段时期里，多数 DNS 服务器都采用一种有章可循的 ID 生成机制，对于每次发送的域名解析请求，DNS 服务器都会将数据包中的 ID 加 1。如此一来，攻击者如果可以在某个 DNS 服务器的网络中进行嗅探，他只要向远程的 DNS 服务器发送一个对本地某域名的解析请求，而远程 DNS 服务器肯定会转而请求本地的 DNS 服务器，于是攻击者可以留心探测目标 DNS 服务器向本地 DNS 服务器发送的请求数据包，就可以得到想要的 ID 号了。

即使攻击者根本无法监听某个拥有 DNS 服务器的网络，也有办法得到目标 DNS 服务器的 ID 号。首先，他向目标 DNS 服务器请求对某个不存在域名地址（但该域是存在的）进行解析。然后，攻击者冒充所请求域的 DNS 服务器，向目标 DNS 服务器连续发送应答包，这些包中的 ID 号依次递增。过一段时间，攻击者再次向目标 DNS 服务器发送针对该域名的解析请求，如果得到了返回结果，就说明目标 DNS 服务器接受了刚才攻击者的伪造应答，继而说明攻击者猜测的 ID 号在正确的区段上，否则，攻击者可以再次尝试。

37. 简述电子邮件欺骗可能造成的危害。

答：攻击者使用电子邮件欺骗有三个目的：

第一，隐藏自己的身份。

第二，如果攻击者想冒充别人，他能假冒那个人的电子邮件。

第三，电子邮件欺骗可被看作是社会工程的一种表现形式。

它造成的危害有：①由于冒充欺骗性，会使得接收邮件人损失金钱和信任关系，虚假的银行提示信息是最常见的恶意邮件或钓鱼攻击类型。攻击者精心设计钓鱼邮件内容，在其中添加较多的官方资源链接和虚假组织的服务链接。通过在邮件中添加合法连接，骗取用户的信任，同时也能成功通过垃圾邮件过滤器的筛选。②损坏邮箱中联系人的资料，泄密隐私。入侵者会收集所有邮件中的用户资料，更严重的是修改邮箱的密码，用户将永远失去这个邮箱的使用权。若是商业用户邮箱被盗窃，则可能造成更大的经济损失。③恶意电子邮件炸弹，会占满系统资源，用户无法接收新邮件，甚至无法使用系统。

38. 试用工具生成一个口令字典。

答：可以采用口令生成软件 GenerateDic 生成一个口令字典，或称为一个单词列表文件。这些单词有的纯粹来自于普通词典中的英文单词，有的则是根据用户的各种信息建立起来的，如用户名字、生日、街道名字、喜欢的动物等。简言之，词典是根据人们设置自己账号口令的习惯总结出来的常用口令列表文件。

我们可以生成一个口令字典，如图 1-3 所示。



图 1-3　口令字典

39. 假定允许使用 26 个字母和 10 个数字构造口令，口令长度为 6 个字符，若采用蛮力攻击，在下列情况下各需要多少时间？

（1）检查一个口令需要 0.1s。

（2）检查一个口令需要 1μs。

答：可能产生口令长度为 6 的口令总数量为 $36\times36\times36\times36\times36\times36=2.1767\times10^9$ 个。

（1）如果检查一个口令的时间为 0.1s，暴力攻击穷举搜索最长结束时间为 2.1767×10^8s，相当于 3627971min，也就是 60466h，等于 2519 天，相当于 6.9 年。

（2）如果检查一个口令需要 1μs 时间，也就是前面单位时间 3627971min 的 10e(−5)，则穷举搜索完毕需要 36.3min。

40. 口令破解有哪些方式？口令破解器通常由哪几部分组成？

答：主要有词典破解、暴力破解或穷举法、组合攻击等方法。还有社会工程学、偷窥、搜索垃圾箱、口令蠕虫、特洛伊木马、网络监听、重放等方法。

口令破解器由候选口令产生器、口令加密模块、口令比较模块三个部分组成。

41. 简述 Windows 下的口令攻击方法有哪些。

答：攻击方法有提取 SAM 文件进行破解、用备份的 SAM 文件替换当前 SAM 文件、使用口令修改软件、替换屏保程序等。

42. 两人试在 UNIX 系统上进行一次口令攻击对抗。

答：原理分析：UNIX 系统用户的口令本来是经过加密后保存在一个文本文件 password 中的，一般存放在/etc 目录下，后来由于安全的需要，把 password 文件中与用户口令相关的域提取出来，组织成文件 shadow，并规定只有超级用户才能读取。这种分离工作也称为 shadow 变换。因此，在破解口令时，需要做 UnShadow 变换，将/etc/password 与/etc/shadow 合并起来，在此基础上才开始进行口令的破解。

现有口令的破解程序如下：

（1）Crack。

Crack 是一个旨在快速定位 UNIX 口令弱点的口令破解程序。Crack 使用标准的猜测技术确定口令。它检查口令是否为如下情况之一：和 user id 相同、单词 password、数字串、字母串。Crack 通过加密一长串可能的口令，并把结果和用户的加密口令相比较，看其是否

匹配。用户的加密口令必须是在运行破解程序之前就已经提供的。

（2）John the Ripper。

UNIX 口令破解程序，但也能在 Windows 平台运行，功能强大、运行速度快，可进行字典攻击和强行攻击。

（3）XIT。

XIT 是一个执行词典攻击的 UNIX 口令破解程序。XIT 的功能有限，因为它只能运行词典攻击，但程序很小、运行很快。

（4）Slurpie。

Slurpie 能执行词典攻击和定制的强行攻击，要规定所需要使用的字符数目和字符类型，如可以用 Slurpie 发起一次攻击，使用 7 字符或 8 字符、仅使用小写字母口令进行强行攻击。

和 John、Crack 相比，Slurpie 最大的优点是它能分布运行，Slurpie 能把几台计算机组成一台分布式虚拟机器在很短的时间里完成破解任务。

43. 举例说明黑客是如何进行 Web 欺骗的。

答：黑客将用户要浏览的网页重定向到黑客自己的服务器，当用户浏览目标网页的时候，实际上是向黑客服务器发出请求，那么黑客就可以达到欺骗的目的。Web 欺骗能够成功的关键是在受害者和真实 Web 服务器之间插入攻击者黑客的 Web 服务器。

例如，2005 年 1 月，一个假冒中国工商银行网站出现在互联网上，真实的中国工商银行网址为：http://www.icbc.com.cn，假冒工商银行网址为 http://www.1cbc.com.cn，黑客诱骗银行卡持有人的账户和密码，并导致多人的银行存款被盗，直接经济损失达 80 万元人民币。

44. 尽可能多地收集 Sniffer 产品的数据，进行比较分析，分别指出它们的使用方法和防范措施。

答：常用的网络 Sniffer（嗅探或称监听）产品有 TcpDump/WinDump、Ngrep、Ethereal /Wireshark、Sniffer Pro 和 NetXray 等。

TcpDump 可以将网络中传送的数据包的“头”完全截获下来提供分析。它支持针对网络层、协议、主机、网络或端口的过滤，并提供 and、or、not 等逻辑语句帮助去掉无用的信息。TcpDump 的总的输出格式为：系统时间，来源主机、端口，目标主机、端口，数据包参数。

Ngrep 是 grep（在文本中搜索字符串的工具）的网络版，它力求更多的 grep 特征，用于搜寻指定的数据包。正由于安装 Ngrep 需用到 libpcap 库，所以支持大量的操作系统和网络协议。Ngrep 能识别 TCP、UDP 和 ICMP 包，理解 BPF 的过滤机制，可用来分析、定位服务中的问题。

Ethereal 是当前较流行的一种计算机网络调试和数据包嗅探软件。Ethereal 基本类似于 TcpDump，但 Ethereal 还具有设计完美的 GUI 和众多分类信息及过滤选项。用户通过 Ethereal，同时将网卡插入混合模式，可以查看到网络中发送的所有通信流量。Ethereal 应用于故障修复、分析、软件和协议开发及教育领域。它具有用户对协议分析器所期望的所有标准特征，并具有其他同类产品不具备的有关特征。Ethereal 可以读取从 TcpDump（libpcap）、网络通

用嗅探器（被压缩和未被压缩）、Sniffer™ 专业版、NetXray™、Sun Snoop 和 atmsnoop、Shomiti/Finisar 测试员、AIX 的 iptrace、Microsoft 的网络监控器、Novell 的 LANalyzer、RadCom 的 WAN/LAN 分析器、ISDN4BSD 项目的 HP-UX nettl 和 i4btrace、Cisco 安全 IDS iplog 和 pppd 日志（pppdump 格式）、WildPacket 的 EtherPeek/TokenPeek/ AiroPeek 或者可视网络的可视 UpTime 处捕获的文件。此外，Ethereal 也能从 Lucent/Ascend WAN 路由器和 Toshiba ISDN 路由器中读取跟踪报告，还能从 VMS 的 TCPIP 读取输出文本和 DBS Etherwatch。

Sniffer Pro 是一款便携式网管和应用故障诊断分析软件，不管是在有线网络，还是在无线网络中，它都能够给予网络管理人员实时的网络监视、数据包捕获以及故障诊断分析能力。对于在现场进行快速的网络和应用问题故障诊断，基于便携式软件的解决方案具备最高的性价比，却能够让用户获得强大的网管和应用故障诊断功能。与 NetXray 比较，Sniffer Pro 支持的协议更丰富，例如，PPPOE 协议等在 NetXray 并不支持，在 SnifferPro 上能够进行快速解码分析。NetXray 不能在 Windows 2000 和 Windows XP 上正常运行，Sniffer Pro 4.6 可以运行在各种 Windows 平台上。Sniffer Pro 的最新版本为 Sniffer Portable Professional 3.0，是取代 Sniffer Pro 4.8/4.9 的最新版本，它提供了 64 位操作系统的支持、无线网络解码和专家分析系统（802.11a/b/g/n）、CDMA 2000、WCDMA 解码和专家分析系统以及大量的细节化协议定制的更新。2009 年，NetScout 在中国设立了专门的 Sniffer 中文官方网站。

NetXray 是由 CincoNetworks 公司开发的一个用于高级分组检错的软件，功能很强大。IP 地址查询工具对硬件要求低，可运行常用的 Windows 平台。它的特点是：①监视网络状态，为优化网络性能提供资料：长时间的捕获，依据统计数值分析网络性能。②网络中包的捕捉和解码，用于故障分析：尽量精确地设置捕捉规则，利于精确分析。③精美的图形化界面、灵活的过滤策略和辅助功能。④捕获并分析数据包，发送数据包，网络管理查看。⑤协议分析软件。⑥运行于数据链路层，对数据帧进行捕捉和分析；此时工作网卡处于混杂模式。⑦可以分析数据链路层及以上的协议和特定用户数据。⑧不能处理物理层协议，如电信号的串扰、衰减等。

因为上述 Sniffer 软件可能被黑客或犯罪使用，为了安全起见，在非网络管理用途的计算机上不应该运行这一类的网络分析软件，为了屏蔽它们，可以屏蔽内核中的 bpfilter 伪设备。一般情况下，网络硬件和 TCP/IP 堆栈不支持接收或发送与本计算机无关的数据包，为了接收这些数据包，就必须使用网卡的混杂模式，并绕过标准的 TCP/IP 堆栈才行。在 FreeBSD 下，这就需要内核支持伪设备 bpfilter。因此，在内核中取消 bpfilter 支持，就能屏蔽 TcpDump 之类的网络分析工具，并且当网卡被设置为混杂模式时，系统会在控制台和日志文件中留下记录，提醒管理员留意这台系统是否被用作攻击同网络的其他计算机的跳板，即监测网卡的工作模式，防御监听软件的侵入。

由于嗅探器是一种被动攻击技术，因此很难被发现。完全主动的解决方案很难找到并且因网络类型而有一些差异，但可以先采用一些被动但却通用的防御措施。这主要包括采用安全的网络拓扑结构和数据加密技术两方面。此外，要注意重点区域的安全防范。

45. 嗅探软件是如何捕捉到数据包并实现数据包过滤功能的？

答：在共享式局域网中，集线器会广播所有数据，这时如果局域网中的一台主机将网卡设置成混杂模式，那么它就可以接收到该局域网中的所有数据了。

如前所述，共享式以太网的传输采取广播实现的方式，即一个局域网中的所有网络接口都有访问在物理媒体上传输的所有数据的能力。但在其正常工作时，只能接收到以本主机为目标主机的数据包，其他数据包过滤后被丢弃。这个过滤机制可以作用在链路层、网络层和传输层等层次。链路层的过滤主要是利用网卡驱动程序判断所接收到的包的目的物理地址（MAC 地址）。系统正常工作时，一个合法的网络接口只响应目标区域和本地网络接口相匹配的硬件地址和目标区域具有“广播地址”的数据帧，它将这些数据帧上交给网络层。其他数据帧将被丢弃，不作处理。在网络层判断目标 IP 地址是否为本机所绑定的 IP 地址，如果是，则将数据包交给传输层处理；如果不是，则丢弃。在传输层判断对应的目标端口是否在本机已经打开，如果已经打开，则根据 TCP/UDP 向应用层提交其内容；如果没有打开，则丢弃。因而，如果没有一个特定的机制，上层应用也无法抓到本不属于自己的“数据包”。

如果要让用户的嗅探软件可以真正“抓”到这些数据包，就需要一个直接与网卡驱动程序接口的驱动模块作为网卡驱动与上层应用的“中间人”，它将网卡设置成混杂模式，并从上层应用（嗅探软件）接收下达的各种抓包请求，对来自网卡驱动程序的数据帧进行过滤，最终将其要求的数据返回给嗅探软件。

可以看到，有了这个“中间人”，链路层的网卡驱动程序上传的数据帧就有了两个去处：一个是正常的 TCP/IP 协议栈；另一个是分组捕获，即过滤模块。对于非本地的数据包，前者会丢弃（通过比较目标 IP 地址），后者则会根据上层应用的要求决定是上传，还是丢弃。链路层两种不同的分组处理模式如图 1-4 所示。

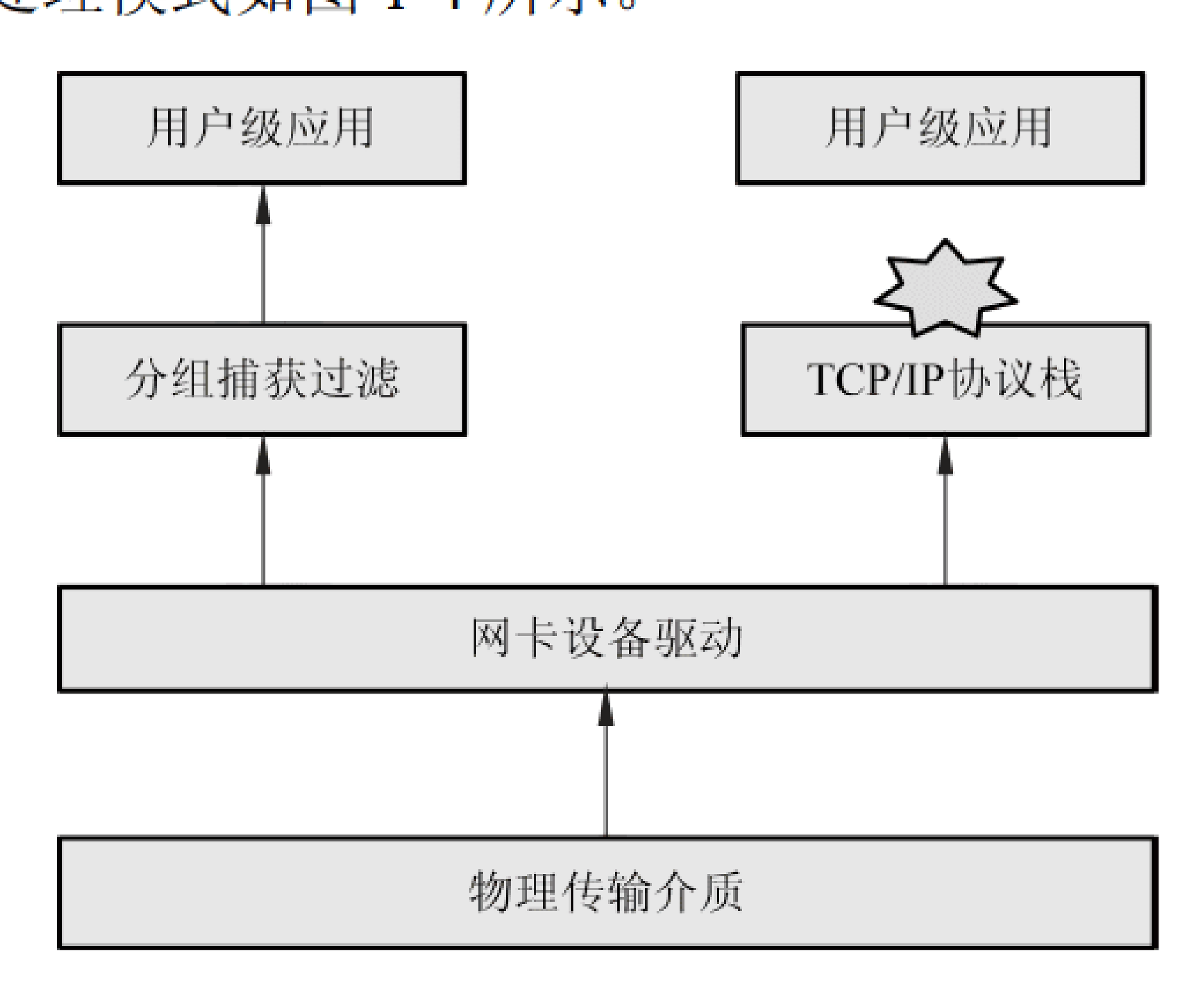


图 1-4　链路层两种不同的分组处理模式

许多操作系统都提供了这样的“中间人”机制，即分组捕获过滤机制。在 UNIX 类型的操作系统中，主要有 3 种：BSD 系统中的 BPF（Berkeley Packet Filter）、SVR4 中的 DLPI（Date Link Provider Interface）和 Linux 中的 SOCK_PACKET 类型套接字。目前，大部分嗅探软件都是基于上述机制建立起来的，利用中间人机制捕捉到数据包并实现数据包过滤功能。

46. 介绍一种扫描工具的用法，记录扫描结果并对扫描结果进行分析。

答：Nmap（Network Mapper）是由 Fyodor 制作的端口扫描工具。

它除了提供基本的TCP和UDP端口扫描功能外，还综合集成了众多扫描技术。可以说，现在的端口扫描技术很大程度上是根据 Nmap 的功能设置划分的。

Nmap还有一个卓越的功能，那就是采用一种叫作“TCP栈指纹鉴别（stack fingerprinting）”的技术探测目标主机的操作系统类型。

使用-sT 选项指定进行 TCP connect 端口扫描（全扫描），如果不指定端口号，默认情况下 Nmap 会扫描 1-1024 和 nmap-services 文件(在 Nmap 下载包中)中列出的服务端口号。图 1-5 是利用-sT 对 192.168.0.1 主机进行 TCP connect 扫描的情况，扫描端口为 TCP21-25、80 以及 139 端口，最终结果显示，21、25、80 和 139 端口是开放的。

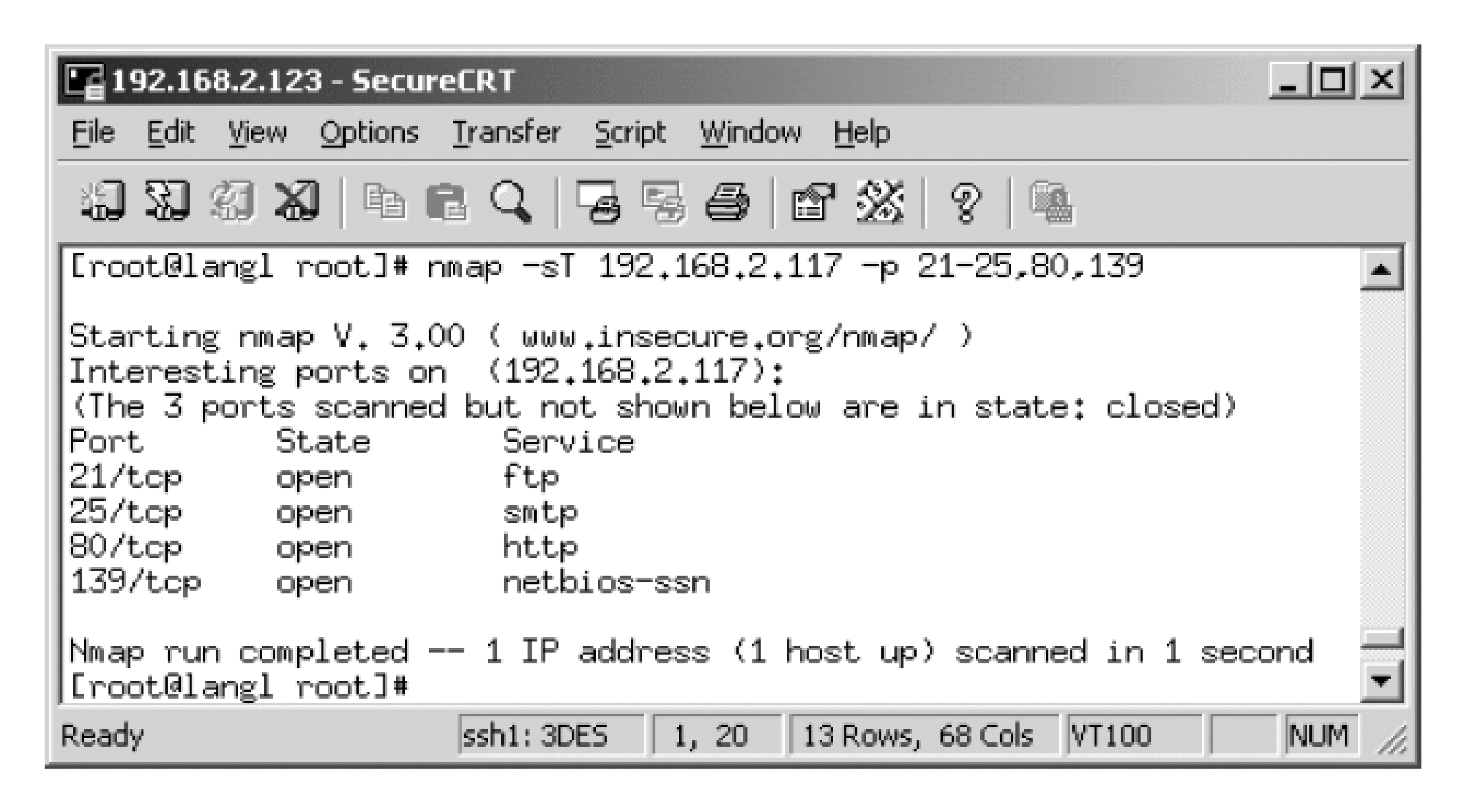


图 1-5　扫描结果显示

47. 请解释全扫描和半扫描的不同。

答：全扫描是攻击者进行端口扫描最常用的方法，就是尝试与远程主机的端口建立一次完整正常的 TCP 连接。如连接成功，则表示端口开放。这种扫描方式也称为“TCP connect 扫描”。

半扫描是指当客户端发出一个 SYN 连接请求报文后，如果收到了远程目标主机的 ACK/SYN 确认，就说明远程主机的该端口是打开的；若没有收到远程目标主机的 ACK/SYN 确认，收到的是 RST 数据报文，就说明远程主机的该端口没有打开。这样，对于扫描要获得的信息已经足够了，由于 SYN 扫描时，全连接尚未完整建立，所以这种技术通常也被称为“半连接或半开放”扫描。全扫描与半扫描的不同在于，前者建立了 TCP/IP 三次握手全连接过程，后者只建立了二次握手半连接过程。全扫描这种扫描方法很容易被检测出来，在日志文件中会有大量密集的连接和错误记录，并容易被防火墙发现和屏蔽，而半扫描即使日志中对于扫描有所记录，但是尝试进行连接的记录也要比全扫描的记录少得多。

48. 秘密扫描是如何实现的？

答：秘密扫描是指 TCP FIN 扫描，通常作用于 UNIX 系统。扫描主机向目标主机发送 FIN 数据包探听端口，若 FIN 数据包到达的是一个打开的端口，数据包则被简单地丢掉，并不返回任何信息，当 FIN 数据包到达一个关闭的端口，TCP 会把它判断成是错误，数据

包会被丢掉，并且会返回一个 RST 数据包，因为此扫描能躲避 IDS、防火墙、包过滤器和日志审计，从而获取目标端口的开放或关闭的信息，因此称为秘密扫描。

49. 主动协议栈指纹识别 OS（操作系统）有哪些方法？

答：主动协议栈指纹识别 OS 的方法有 FIN 探测，ISN 采样探测，Don't Fragment 位探测，TCP 初始窗口的大小检测，ACK 值探测，ICMP 出错消息抑制，ICMP 出错消息回射完整性，TOS 服务类型和片段处理等。

50. 常用的扫描工具有哪些？

答：常用的扫描工具有：

（1）SATAN（古老经典）。

（2）Nessus（最好的开放源代码风险评估工具）。

（3）Nikto（一款非常全面的 Web 扫描器）。

（4）NMAP（扫描之王）。

（5）SAINT（安全管理员的综合网络工具）。

（6）SARA（安全管理员的辅助工具）。

（7）SuperScan（Windows 平台上的 TCP 端口扫描器）。

（8）Mysfind（漏洞扫描）。

（9）X-Scan（漏洞扫描）。

（10）流光（中国软件）等。

51. 如何对扫描进行防御？

答：防御扫描可以从以下八个方面入手。

（1）减少开放端口，做好系统防护。

（2）实时监测扫描，及时做出告警。

（3）伪装知名端口，进行信息欺骗。

（4）采用端口扫描监测软件，如 ProtectX、Winetd、DTK 蜜罐工具和 PortSentry 等。

（5）采用个人防火墙技术。

（6）采用针对 Web 服务的日志审计技术等。

（7）修改 Banner 信息。

（8）及时更新安全补丁程序等方法。

52. 什么是缓冲区？什么是缓冲区溢出？

答：缓冲区是包含相同数据类型实例的一个连续的计算机内存块，是程序运行期间在内存中分配的一个连续的区域，用于保存包括字符数组在内的各种数据类型。所谓缓冲区溢出，就是所填充的数据超出了原有的缓冲区边界。

53. 下载一个进行缓冲区溢出攻击的程序，并进行分析。

答：

```
/ * File heap1.c * /
# include < stdio.h >
# include < stdlib.h >
# include < unistd.h >
# include < string.h >
# define BUFFER-SIZE 16
# define OVERLAYSIZE 8  /* 覆盖buf2 的前 OVERLAYSIZE 字节 */
int main()
{
u-long diff ;
char * buf1 = (char * )malloc (BUFFER-SIZE) ;
char * buf2 = (char * )malloc (BUFFER-SIZE) ;
diff = (u-long) buf2 - (u-long) buf1 ;
printf ("buf1 = %p , buf2 = %p , diff = 0x %x ( %d) bytes \n", buf1 , buf2 , diff , diff) ;
/* 将buf2 用'a'填充 */
memset (buf2 , 'a', BUFFER-SIZE - 1) , buf2[BUFFER-SIZE - 1 ] = '\0';
printf ("before overflow: buf2 = %s \n", buf2) ;
/* 用diff + OVERLAYSIZE 个'b'填充buf1 */
memset (buf1 , 'b', (u-int) (diff + OVERLAYSIZE) ) ;
printf ("after overflow: buf2 = %s \n", buf2) ;
return 0 ;
}
```

上述程序的运行结果存在缓冲区堆溢出。

可以看到，buf2 的前 8B 被覆盖了，这是因为往 buf1 中填写的数据超出了它的边界，进入了 buf2 的范围。由于 buf2 的数据仍然在有效的 Heap 区内，所以程序仍然可以正常结束。

我们注意到，虽然 buf1 和 buf2 是相继分配的，但它们并不是紧挨着的，而是有 8B 间距。这是因为，使用 malloc()动态分配内存时，系统向用户返回一个内存地址，实际上在这个地址前面通常还有 8B 的内部结构，用来记录分配的块长度、上一个堆的字节数以及一些标志等。这个间距可能随系统环境的不同而不同。buf1 溢出后，buf2 的前 8B 也被改写为 bbbbbbbb，buf2 内部的部分内容也被修改为 b。程序运行结果如图 1-6 所示。

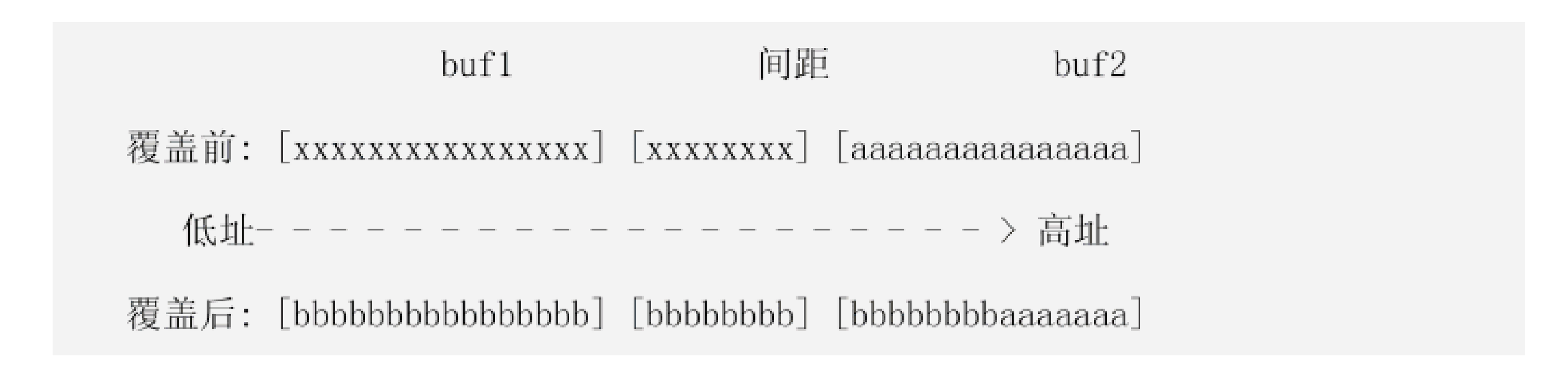


图 1-6　程序运行结果

54. 试举几个利用缓冲区溢出进行攻击的病毒名。简述缓冲区溢出攻击的过程。

答：2004 年 5 月爆发的“震荡波”蠕虫病毒，利用了 Windows 系统的活动目录服务缓冲区溢出漏洞。

2005 年 8 月，利用 Windows 即插即用缓冲区溢出漏洞的“狙击波”蠕虫病毒，被称为

历史上最快利用微软漏洞进行攻击的恶意代码。

2008 年底至 2009 年的 Conficker 蠕虫病毒利用的是 Windows 处理远程 RPC 请求时的漏洞（MS08-067）。

攻击者要实现缓冲区溢出攻击，必须完成两个任务：一是在程序的地址空间里安排适当的代码；二是通过适当的初始化寄存器和存储器，让程序跳转到安排好的地址空间执行。因此，对于攻击者来说，需要构造执行的代码 Shellcode，并将其放到目标系统的内存，然后获得缓冲区的大小和定位溢出点 ret 的位置，最后控制程序跳转，改变程序流程。

55. 简述缓冲区溢出攻击的防御方法。

答：（1）源码级保护方法，包括避免源码中的相关 bug、源码中溢出 bug 的查找和数组边界检查编译器。

（2）运行期保护方法，包括插入目标代码进行数组边界检查、返回指针的完整性检查。

（3）阻止攻击代码执行，具体采用非执行缓冲区技术，通过设置缓冲区地址空间的属性为不可执行，使得攻击代码不能执行，从而避免攻击，这种技术被称为非执行的缓冲区技术。

（4）加强系统保护，具体有保护系统信息、关闭不需要的服务、最小权限原则、使用系统的堆栈补丁、检查系统漏洞、及时为软件打上安全补丁。

56. 阅读下面的程序，指出其功能。

```
#include <stdio.h>
int main(int argc,char *argv[])
{
        unsigned    char     carnary[5];
        unsigned    char     foo[4];
        memset(foo,'\x00',sizeof(foo));
        strcpy(camary,"XXXX");

        fprintf (stderr, "%16u%n%16u%n%32%n%64u%n\n",
                (int *) &foo[0],1,(int*) &foo[1],1 ,(int*) &foo[2],1, (int*) &foo[3]);
        printf ("foo | carmary: %02x%02x%02x%02x | %02x%02x%02x%02x\n",
                foo[0],foo[1],foo[2],foo[3],
                camary[0], camary[1], camary[2], camary[3) ;
}
```

答：运行结果存在格式化串溢出。

格式化串溢出源自*printf()类函数的参数格式问题（如 printf、fprintf、sprintf 等），以最简单的 printf()函数为例：

```
int printf (const char *format, arg1, arg2, …);
```

它们将根据 format 的内容（%s，%d，%p，%x，%n，…）将数据格式化后输出。其问题在

于，*printf()函数并不能确定数据参数 arg1，arg2，…究竟在什么地方结束，即函数本身不知道参数的个数，而只会根据 format 中打印格式的数目依次打印堆栈中参数 format 后面地址的内容。

在 format 串中，主要利用%n 实现攻击，%n 在格式化串中的意思是将显示内容的长度输出到一个变量中。

段错误的原因是 printf()将堆栈中 main()函数的变量 num 当作%n 对应的参数，因此会将 0x14 保存到地址 0x61616161 中，而 0x61616161 是不能访问的地址，因此系统提示发生段错误。如果可以控制 num 的内容，就意味着可以修改任意地址（当然，是允许写入的地址）的内容。

从以上可以看出，缓冲区溢出的真正原因在于程序缺少边界检查。这一方面是源于编程语言和库函数本身的弱点，如 C 语言中对数组和指针的引用不自动进行边界检查，一些字符串处理函数（如 strcpy、sprintf 等）存在着严重的安全问题。另一方面是程序员进行程序编写时，由于经验不足或粗心大意，没有进行或忽略了边界检查，使得缓冲区溢出漏洞几乎无处不在，为缓冲区溢出攻击留下了隐患。

57. 在实验室中模拟一次 SYN Flood 攻击的实际过程。

答：略。

58. 什么是拒绝服务攻击？

答：拒绝服务攻击通常是利用传输协议的漏洞、系统存在的漏洞、服务的漏洞，对目标系统发起大规模的进攻，用超出目标处理能力的海量数据包消耗可用系统资源、带宽资源等，或造成程序缓冲区溢出错误，致使其无法处理合法用户的正常请求，无法提供正常服务，最终致使网络服务瘫痪，甚至引起系统死机。

59. 简要回答拒绝服务攻击有哪些常用技术？各种技术的特点分别是什么？

答：（1）Ping of Death：该攻击数据包大于 65535B。由于部分操作系统接收到长度大于 65535B 的数据包时，会造成内存溢出、系统崩溃、重启、内核失败等后果，从而达到攻击的目的。

（2）泪滴（Teardrop）：“泪滴”也称为分片攻击，它是一种典型的利用 TCP/IP 的漏洞进行拒绝服务攻击的方式。两台计算机在使用 IP 通信时，如果传输的数据量较大，无法在一个数据报文中传输完成，就会将数据拆分成多个分片，在传送到目标计算机后再到堆栈中进行重组，这一过程称为分片（fragmentation）。IP 分片发生在要传输的 IP 报文大小超过最大传输单位（Maximum Transmission Unit，MTU）的情况。

在互联网中，各 IP 分片报文被分别传输，通过的线路不一定相同，到达目标主机的顺序也不一致，为了能在到达目标主机后顺利进行数据重组，各分片报文具有如下信息。

IP 分片识别号（IP identification number，fragment ID）分片在原始报文中的偏移量、分片数据长度、分片标志位（More Fragment，ME），当其后还存在后续分片报文时，将该分片 ME 标志位置为 1。如果攻击者伪造数据报文向服务器发送含有重叠偏移信息的分片包，

当这些含有重叠偏移信息的分片报文被发送到目标主机后，目标主机在堆栈中重组原始数据包时会出错，这个错误不仅会影响重组的数据，还会导致内存错误，引起协议栈的崩溃。

（3）IP 欺骗：这种攻击利用 IP 头的 RST 位实现。假设现在有一个合法用户（61.61.61.61）已经同服务器建立了正常的连接，攻击者构造 TCP 数据包，伪装自己的 IP 为 61.61.61.61，并向服务器发送一个带有 RST 位的 TCP 数据包。服务器接收到这样的数据后，认为从 61.61.61.61 发送的连接有错误，就会清空缓冲区中建立好的连接。这时，如果合法用户 61.61.61.61 再发送合法数据，服务器就已经没有这样的连接了，该用户就必须重新开始建立连接。攻击者利用这一点，构造大量的源地址为其他用户 IP 地址、RST 位置 1 的数据包发送给目标服务器，使服务器不对合法用户服务，从而实现对受害服务器的拒绝服务攻击。

（4）UDP 洪水：利用主机能自动进行回复的服务（例如，使用 UDP 的 chargen 服务和 echo 服务）进行攻击。

（5）SYN 洪水：这是一种利用 TCP 缺陷发送大量伪造的 TCP 连接请求，使被攻击方资源耗尽(CPU 满负荷或内存不足)的攻击方式。

（6）Land 攻击：构造一个特殊的 SYN 包，其源地址和目标地址相同。

（7）Smurf 攻击：当某台机器使用广播地址发送一个 ICMP echo 请求包时（如 Ping），它就会收到 N 个 ICMP echo 回应包（N 为网络中计算机的总数）。当 N 的数目达到一定大小时，产生的应答流量将会占用大量的带宽，消耗大量的网络资源。Smurf 攻击就是使用这个原理进行的。Smurf 攻击在构造数据包时将源地址设置为被攻击主机的地址，而将目标地址设置为广播地址，于是，大量的 ICMP echo 回应包被发送给被攻击主机，使其因网络阻塞而无法提供服务。

（8）Fraggle 攻击：Fraggle 攻击原理与 Smurf 一样，也是采用向广播地址发送数据包，利用广播地址的特性将攻击放大，以使目标主机拒绝服务。不同的是，Fraggle 使用的是 UDP 应答消息，而非 ICMP 数据包。

（9）电子邮件炸弹：电子邮件炸弹是最古老的匿名攻击之一，简言之，就是攻击者不停地向用户的邮箱发送大量的邮件，目的是用垃圾邮件填满你的邮箱，使正常的邮件因邮箱空间不够而被拒收。这也将不断吞噬邮件服务器上的硬盘空间，最终耗尽，无法再对外服务。

（10）畸形消息攻击：畸形消息攻击是一种有针对性的攻击方式，它利用目标主机或者特定服务在处理接收到的信息之前没有进行适当的信息错误检验，故意发送一些畸形消息，使目标主机出现处理异常或崩溃。

（11）Slashdot effect：由于 Slashdot.org 的知名度和浏览人数的影响，在 Slashdot.org 上的文章中放入的网站链接有可能一瞬间被点入上千次，甚至上万次，造成这个被链接的网站承受不住突然增加的连接请求，出现响应变慢、崩溃、拒绝服务。这种现象就称为 Slashdot effect，这种瞬间产生的大量进入某网站的动作，也称 Slashdotting。

（12）WinNuke 攻击：WinNuke 攻击又称“带外传输攻击”，它的特征是攻击目标端口，被攻击的目标端口通常是 139、138、137、113、53。TCP（传输控制协议）中使用带外数据（OOB 数据）通道传送一些比较特殊（如比较紧急）的数据，当发送方使用这一方式时，发送方 TCP 进入紧急模式。WinNuke 攻击就是制造特殊的这种报文，它们与正常带外数据

报文不同的是，它们的 URG 指针字段与数据的实际位置不符，即存在重合，这样，Windows 操作系统在处理这些数据的时候就会出现错误，造成系统崩溃。

60. 如何防御拒绝服务攻击对系统的危害？

答：（1）优化网络和路由结构。

（2）保护主机系统安全。

（3）安装入侵检测系统。

（4）与因特网服务供应商（ISP）合作。

（5）使用扫描工具。

61. 在 DDoS 攻击中，为什么黑客不直接控制攻击傀儡机，而要通过控制傀儡机发动进攻呢？

答：傀儡机是分布式拒绝服务攻击（Distributed Denial of Service attack，DDoS）中的概念，攻击者通过控制分布在网络各处的数百甚至数千台傀儡主机（又称为肉鸡），发动它们同时向攻击目标进行拒绝服务攻击。

僵尸网络可以用作傀儡机平台，就是攻击者手中的一个攻击平台，由互联网上数百到数十万计算机构成，这些计算机被黑客利用蠕虫等手段植入了僵尸程序并暗中操控。利用这样的攻击平台，攻击者可以实施 DDoS 攻击，并且反过来创建新的僵尸网络，进一步扩大其控制范围，威力之大，远非 DoS 攻击手段可比。

DDoS 攻击通常借助客户/服务器技术。在进行 DDoS 攻击前，攻击者必须先用其他手段获取大量傀儡主机的系统控制权，用于安装进行拒绝服务攻击的软件。这些傀儡主机最好具有良好的性能和充足的资源，如强的计算能力和大的带宽等。

用于 DDoS 攻击的软件一般分为守护端（安装守护端的主机称为代理）与服务端（安装服务端的主机称为主控）。这些程序可以协调使分散在互联网各处的机器共同完成对一台主机的攻击操作。

当需要攻击时，攻击者连接到安装了服务端软件的主控，向服务端软件发出攻击指令，主控在接收到攻击指令后，控制多个代理同时向目标主机发动猛烈攻击。通常，主控与代理之间并不是一一对应的关系，而是多对多的关系。也就是说，一个安装了代理的服务器可以被多个主控所控制，一个主控也同时控制多个代理。

采用这种三层结构，黑客不直接控制攻击傀儡机，而要通过控制傀儡机发动进攻确保黑客的安全。黑客发出指令后，就可以断开连接，由主控负责指挥代理展开攻击。因此，黑客连接网络和发送指令的时间很短，隐蔽性极强，不易被防御，导致 DDoS 攻击难以被追查。从攻击者的角度来说，肯定不愿意被捉到，而攻击者使用的傀儡机越多，他实际上提供给受害者的分析依据就越多。在占领一台机器后，高水平的攻击者首先会做两件事：①考虑如何留好后门；②如何清理日志。这就是擦掉脚印，不让自己做的事被别人察觉到。比较不敬业的黑客会把日志全都删掉，但这样的话，网络管理员一旦发现日志都没了，就会知道有人干了坏事，顶多无法再从日志发现是谁干的而已。相反，真正的高手会挑有关自己的日志项目删掉，让人看不到异常的情况。这样可以长时间地利用傀儡机。

但是，在攻击傀儡机上清理日志实在是一项庞大的工程，即使在有很好的日志清理工具的帮助下，黑客对这个任务也是很头痛的。这就导致有些攻击机弄得不是很干净，通过它上面的线索找到了控制它的上一级计算机，上一级的计算机如果是黑客自己的机器，那么他就会被揪出来了。但如果这是控制用的傀儡机，黑客自身还是安全的。控制傀儡机的数目相对很少，一般一台就可以控制几十台攻击机，清理一台计算机的日志对黑客来讲轻松多了，这样，从控制机再找到黑客的可能性也大大减小。

62．在 http://www.fbi.gov/nipc/trinoo.htm 上有一个检测和根除 trinoo 的自动程序。请下载并试用一次。

答：trinoo 是基于 UDPflood 的攻击软件，它向被攻击目标主机随机端口发送全零的 4B UDP 包，被攻击主机的网络性能在处理这些超出其处理能力垃圾数据包的过程中不断下降，直至不能提供正常服务，甚至崩溃。

63. trinoo DDoS 有如下一些基本特性，请根据这些特性提出抵御 trinoo 的策略。

（1）在主控（master）程序与代理程序的所有通信中，trinoo 都使用了 UDP。

（2）trinoo master 程序的监听端口是 27655，攻击者一般借助 Telnet 通过 TCP 连接到 master 程序所在的计算机。

（3）所有从 master 程序到代理程序的通信都包含字符串“l44”，并且被引导到代理的 UDP 端口 27444。

（4）master 和代理之间通信受到口令的保护，但是口令不是以加密格式发送的，因此它可以被“嗅探”到并被检测出来。

答：DoS（Denial of Service）即拒绝服务。造成 DoS 攻击行为的被称为 DoS 攻击，其目的是使计算机或网络无法提供正常的服务。最常见的 DoS 攻击有计算机网络带宽攻击和连通性攻击。DoS 攻击是指故意的攻击网络协议实现的缺陷或直接通过野蛮手段耗尽被攻击对象的资源，让目标计算机或网络无法提供正常的服务或资源访问，使目标系统、服务系统停止响应，甚至崩溃，而在此攻击中并不包括侵入目标服务器或目标网络设备。这些服务资源包括网络带宽、文件系统空间容量、开放的进程或者允许的连接。这种攻击会导致资源匮乏，无论计算机的处理速度多快、内存容量多大、网络带宽的速度多快，都无法避免这种攻击带来的后果。

trinoo 是复杂的 DDoS 攻击程序，它使用 master 程序对实际实施攻击的任何数量的“代理”程序实现自动控制。攻击者连接到安装了 master 程序的计算机，启动 master 程序，然后根据一个 IP 地址的列表，由 master 程序负责启动所有的代理程序。接着，代理程序用 UDP 信息包冲击网络，从而攻击目标。在攻击之前，侵入者为了安装软件，已经控制了装有 master 程序的计算机和所有装有代理程序的计算机。

下面是 trinoo DDoS 攻击的基本特性以及建议采用的抵御策略。

（1）在 master 程序与代理程序的所有通信中，trinoo 都使用了 UDP。入侵检测软件能够寻找使用 UDP 的数据流（类型 17）。

（2）trinoo master 程序的监听端口是 27655，攻击者一般借助 telnet 通过 TCP 连接到

master 程序所在的计算机。入侵检测软件能够搜索到使用 TCP（类型 6）并连接到端口 27655 的数据流。

（3）所有从 master 程序到代理程序的通信都包含字符串“l44”，并且被引导到代理的 UDP 端口 27444。入侵检测软件检查到 UDP 端口 27444 的连接，如果有包含字符串 l44 的信息包被发送过去，那么接收这个信息包的计算机可能就是 DDoS 代理。

（4）master 和代理之间通信受到口令的保护，但是口令不是以加密格式发送的，因此它可以被“嗅探”到并被检测出来。使用这个口令以及来自 Dave Dittrich 的 trinot 脚本，要准确地验证出 trinoo 代理的存在是很可能的。

一旦一个代理被准确地识别出来，trinoo 网络就可以按照如下步骤被拆除。

A. 在代理 daemon 上使用 strings 命令，将 master 的 IP 地址暴露出来。

B. 与所有作为 trinoo master 的机器管理者联系，通知它们这一事件。

C. 在 master 计算机上识别含有代理 IP 地址列表的文件（默认名为“...”），得到这些计算机的 IP 地址列表。

D. 向代理发送一个伪造 trinoo 命令禁止代理。通过 crontab 文件（在 UNIX 系统中）的一个条目，代理可以有规律地重新启动，因此，代理计算机需要一遍一遍地被关闭，直到代理系统的管理者修复了 crontab 文件为止。

E. 检查 master 程序的活动 TCP 连接，这能显示攻击者与 trinoo master 程序之间存在的实时连接。

F. 如果网络正在遭受 trinoo 攻击，那么系统就会被 UDP 信息包所淹没。trinoo 从同一源地址向目标主机上的任意端口发送信息包。探测 trinoo 就是要找到多个 UDP 信息包，它们的特点是使用同一来源 IP 地址、同一目标 IP 地址、同一源端口和不同的目标端口。

G. 在美国 FBI 网站上下载检测和根除 trinoo 的自动程序。

64. 在网络上下载 2～3 个 DDoS 监测软件，安装到自己的机器上，记录其工作过程。

答：（1）V1.0 幽幽 DDoS 攻击探测器下载，实时监控 DDoS 攻击流量，下载地址为 http://www.cr173.com/soft/9245.html。

（2）中新金盾防火墙 DDoS 攻击监测工具的下载网址为 http://dl.pconline.com.cn/download/614714.html。

65. 总结 DDoS 攻击的防御方法。

答：DDoS 攻击的防御有两种方式：一种是直接在高防机房架设服务器，做一个跳转，直接隐藏真实 IP；另一种是选择内容分发网络（Content Delivery Network，CDN），直接将攻击分配到各个 CDN 点上。

总体来说，对 DoS 和 DDoS 的防范主要从下面几个方面考虑：

尽可能对系统加载最新补丁，并采取有效的合规性配置，降低漏洞利用风险；

采取合适的安全域划分，配置防火墙、入侵检测和防范系统，减缓攻击。采用分布式组网、负载均衡、提升系统容量等可靠性措施，增强总体服务能力。

可参考的具体措施如下。

（1）采用高性能的网络设备。

首先，保证网络设备不能成为瓶颈，因此选择路由器、交换机、硬件防火墙等设备时要尽量选用知名度高、口碑好的产品。其次，如果和网络提供商有特殊关系或协议就更好了，当大量攻击发生时，请他们在网络接点处做一下流量限制，对抗某些种类的 DDoS 攻击是非常有效的。

（2）尽量避免 NAT 的使用。

无论是路由器，还是硬件防护墙设备，要尽量避免采用网络地址转换（NAT）的使用，因为采用此技术会较大降低网络通信能力。原因很简单，因为 NAT 需要对地址来回转换，转换过程中需要对网络包的校验和进行计算，因此浪费了很多 CPU 的时间，但有些时候必须使用 NAT，那就没有好办法了。

（3）充足的网络带宽保证。

网络带宽直接决定了能抗受攻击的能力，假若仅有 10Mb/s 带宽，无论采取什么措施都很难对抗当今的 SYN Flood 攻击，至少要选择 100Mb/s 的共享带宽，最好的当然是挂在 1000Mb/s 的主干上了。但需要注意的是，主机上的网卡是 1000Mb/s 的并不意味着它的网络带宽就是千兆的，若把它接在 100Mb/s 的交换机上，它的实际带宽不会超过 100Mb/s，再就是接在 100Mb/s 的带宽上也不等于就有了百兆的带宽，因为网络服务商很可能会在交换机上限制实际带宽为 10Mb/s，这一点一定要搞清楚。

（4）升级主机服务器硬件。

在有网络带宽保证的前提下，请尽量提升硬件配置，要有效对抗每秒 10 万个 SYN 攻击包，服务器的配置至少应该为：P4 2.4GHz/DDR512MB/SCSI-HD，起关键作用的主要是 CPU 和内存，内存一定要选择 DDR 的高速内存，硬盘要尽量选择 SCSI 的，别贪 IDE 价格低量还足的便宜，否则会付出高昂的性能代价，再就是一定要选用 3COM 或 Intel 等名牌的网卡，若是 Realtek 的，还是用在自己的 PC 上吧。

（5）把网站做成静态页面。

大量事实证明，把网站尽可能做成静态页面，不仅能大大提高抗攻击能力，而且还给黑客入侵带来不少麻烦，至少到目前为止，关于 HTML 的溢出还没出现，新浪、搜狐、网易等门户网站主要都是静态页面，若你一定需要动态脚本调用，那就把它放到另外一台单独主机，以免遭受攻击时连累主服务器。当然，适当放一些动态脚本不做数据库调用脚本还是可以的。此外，最好在需要调用数据库的脚本中拒绝使用代理的访问，因为经验表明，使用代理访问网站的 80%属于恶意行为。

（6）软件定义网络（Software Defined Network, SDN）技术在安全防护方面的优势。

SDN 将网络控制平面与网络传输平面分离出来，由集中式控制器控制管理整个网络的数据转发和处理功能，其多粒度网络分析能力可以高效地提供实时网络状态信息，为网络运维人员快速发现和识别异常流量提供便利。

SDN 灵活可调度提高安全响应速度。SDN 技术将物理资源进行虚拟化，并利用其可编程的特点为运维人员提供快速调整资源部署和流量调度的能力，在发现攻击行为或者流量

异常时可以在第一时间制订相应的策略并下发至各个网络节点，进行流量阻断或重定向清洗。另外，当面对超出现有处理能力的安全攻击时，还可以快速将防护资源或者带宽资源向被攻击网络进行调配，以便满足安全防御和业务保证的需求。

SDN 服务开放性可提供联动接口和定制化服务，SDN 架构中北向接口的开放性支持引入第三方的流量检测和清洗虚拟功能模块，也支持与其他系统的联动交互，而且还可以根据客户提出的实际需求提供定制化异常流量清洗服务，如清洗的带宽、清洗的触发条件、清洗的内容等。

SDN 部署成本较低有利于全网推广部署。SDN 的虚拟化能力使得在安全系统部署实施中只须使用通用的硬件服务器，并安装不同虚拟机软件即可具备防护功能，从而实现硬件设备的共享复用。另外，通过对虚拟化能力的智能化编排，可以实现按需分配防护资源，并对全网流量进行调度牵引，避免冗余备份、减少建设成本和运维成本。

66．浏览 3 个黑客网站，综述黑客们讨论的热点问题。

答：黑客常用网站如图 1-7 所示。



图 1-7　黑客常用网站

讨论的热点问题有系统漏洞、分布式拒绝服务攻击、破解口令及安全防御等。

67. 信息系统为什么会存在攻击？试从硬件和软件两方面加以回答。

答：信息系统存在攻击是系统自身的脆弱性导致的，其中包括硬件和软件两方面的脆弱。信息系统的硬件脆弱性来自设计上的不完善和有限寿命，软件组件的脆弱性来源于设计和软件工程实施中遗留的问题，软件设计中的疏忽，软件设计中不必要的功能冗余、软

件过长过大，软件设计不按信息系统安全等级要求进行模块化设计以及软件工程实现中造成的软件系统内部逻辑混乱等。

68. 黑客攻击信息系统有哪些方法？

答：网络黑客的主要攻击手法有：获取口令、放置木马病毒软件、Web 欺骗技术、电子邮件攻击、通过一个节点攻击另一节点、网络监听、寻找系统漏洞、利用缓冲区溢出窃取特权等。

第 2 章　数据安全保护

2.1　第 2 章知识提要

本章详细讲解数据保护，包括数据加密解密基础、对称和非对称密码体制、数据加密的国际标准消息认证 DES、AES、数字签名的国际标准 DSA、电子商务交易 SET 的主要流程等。

2.2　第 2 章习题和答案详解

一、选择题（答案：ACCBA CD）

1. 假设使用一种加密算法，它的加密方法很简单：将每一个字母加5，即a加密成f。这种算法的密钥就是5，那么它属于 ________。
   A. 对称加密技术
   B. 分组密码技术
   C. 公钥加密技术
   D. 单向函数密码技术

答案：A

解答： 对称密码是指加密密钥和解密密钥相同，因此选A。

2. “公开密钥密码体制”的含义是________。
   A. 将所有密钥公开
   B. 将私有密钥公开，公开密钥保密
   C. 将公开密钥公开，私有密钥保密
   D. 两个密钥相同

答案：C

解答： 公开密钥体制的定义是公钥公开，私钥保密，因此选C。

3. A方有一对密钥($K_{A公}, K_{A秘}$)，B方有一对密钥($K_{B公}, K_{B秘}$)，A方向B方发送数字签名M，对信息M加密为：$M' = K_{B公}(K_{A秘}(M))$。B方收到密文的解密方案是________。
   A. $K_{A公}(K_{A秘}(M'))$
   B. $K_{A公}(K_{A公}(M'))$
   C. $K_{A公}(K_{B秘}(M'))$
   D. $K_{B秘}(K_{A秘}(M'))$

答案：C

解答：解密方案是加密的逆运算，因此选C。

4. 使用数字签名技术，在发送端，它是采用________对要发送的信息进行数字签名的。
   A．发送者的公钥
   B．发送者的私钥
   C．接收者的公钥
   D．接收者的私钥

答案：B

解答：数字签名是用发送者的私钥对数字进行加密，因此选B。

5. 使用数字签名技术，在接收端，采用________进行签名验证。
   A．发送者的公钥
   B．发送者的私钥
   C．接收者的公钥
   D．接收者的私钥

答案：A

解答：数字签名的验证是使用发送者的公钥进行验证，因此选A。

6. 数字签名要预先使用单向Hash函数进行处理的原因是________。
   A. 多一道加密工序，使密文更难破译
   B. 提高密文的计算速度
   C. 缩小签名密文的长度，加快数字签名和验证签名的运算速度
   D. 保证密文能正确还原成明文

答案：C

解答：只有C最符合题中的描述。

7. 设哈希函数H的输出长度为128位，如果H的k个随机输入中至少有两个产生相同输出的概率大于0.5，则k约等于________。
   A．2^{128}
   B．2^{64}
   C．2^{32}
   D．2^{256}

答案：D

解答：128的2倍等于256，因此选D。

二、填空题

答案：1. 明文空间，密文空间，密钥空间，密码算法

2. 解密算法 D
3. 对称密码
4. RSA
5. 传送密钥，数字签名
6. 生成，分配，使用，保护，存储，更新，销毁
7. 人为设定生成，自动密钥设备生成
8. 用户
9. KDC
10. 消息的完整性
11. 数字签名
12. 安全电子交易（SET）协议
13. 不要求可逆性
14. 哈希函数

1. 密码系统包括以下4个方面：明文空间、密文空间、密钥空间和密码算法。
2. 解密算法D是加密算法E的逆运算。
3. 如果加密密钥和解密密钥相同，则这种密码体制称为对称密码体制。
4. RSA 算法的安全是基于分解两个大素数的积的困难。
5. 公开密钥加密算法的用途主要包括两个方面：传送密钥、数字签名。
6. 密钥管理的主要内容包括密钥的生成、分配、使用、保护、存储、更新和销毁。
7. 密钥生成形式有两种：一种是由人为设定生成，另一种是由自动密钥设备生成。
8. 密钥的分配是指产生并使用户获得密钥的过程。
9. 密钥分配中心的英文缩写是KDC。
10. 消息认证是验证消息的完整性，即验证数据在传送和存储过程中是否被篡改、重放或延迟等。
11. 数字签名是笔迹签名的模拟，是一种包括防止源点或终点否认的认证技术。
12. 安全电子交易（SET）协议是实现交易安全的核心技术之一，它的实现基础就是加密技术，能够实现电子文档的辨认和验证。
13. MAC函数类似于加密，它与加密的区别是其不要求可逆性。
14. 哈希函数是可接受变长数据输入，并生成定长数据输出的函数。

三、问答题

1. 有明文 can you understand，

（1）假定有一个密钥，其顺序为 2，4，3，1 的列换位密码，其换位密文是什么？

（2）设密钥是 i=1，2，3，4 的一个置换 $f(i)$=1，3，4，2，则周期为 4 的换位密文是什么？

答：（1）首先，4 位分成 4 列 4 行矩阵，按行输入

2431

```
cany
ouun
ders
tand
```

按照题中给定的换位密码规则：2,4,3,1，列表如下。

密钥序列号	2	4	3	1
明文	c	a	n	y
	o	u	u	n
	d	e	r	s
	t	a	n	d

也就是首先读出的是第四列，按密钥的列顺序读出，得其换位密文为

ynsd codt nurn auea

（2）codt ynsd auea nurn。

2. 设 P = blue sky and green tree，密钥 K=data，则采用维吉尼亚密码的加密字母是什么？ASCII 编码的输出为什么？

答：加密字母是 ELNE VKR AQD ZRHEG TUEX，十进制 ASCII 编码输出是 69 76 78 69 86 75 82 65 81 68 90 82 72 69 71 84 85 69 88，十六进制 ASCII 编码输出是 45 4C 4E 45 56 4B 52 41 51 44 5A 52 48 45 47 54 55 45 58，二进制 ASCII 编码输出是 01000101 01001100 01001110 01000101 01010110 01001011 01010010 01000001 01010001 01000100 01011010 01010010 01001000 01000101 01000111 01010100 01010101 01000101 01011000

3. 比较两种密钥体制的优缺点。

答：这里，两种密钥体制是指对称密码体制和非对称密码体制。对称密码体制是指加密密钥和解密密钥相同，著名的有 DES、AES 算法等。非对称密码体制是指加密密钥和解密密钥不相同，或者说不能由其中一个密钥推导出另一个密钥，著名的有 RSA 算法等。

对称密码体制的优点在于效率高、加解密速度快、密钥较短、发展历史悠久、算法简单、系统开销小、适合加密大量数据。

缺点如下。

（1）密钥是保密通信的关键，发信方必须安全、妥善地把密钥送到收信方，不能泄露其内容，密钥的传输必须安全，如何才能把密钥安全送到收信方是对称加密体制的突出问题。

（2）n 个合作者就需要 n 个不同的密钥，如果 n 个人两两通信需要密钥的数量为 $n(n-1)$，则使得密钥的分发复杂。

（3）通信双方必须统一密钥，才能发送保密信息，如果双方不相识，就无法向对方发送秘密信息了。

（4）难以解决电子商务系统中的数字签名认证问题。对开放的计算机网络，存在着安全隐患，不适合网络邮件加密需要。

非对称密码体制加密算法复杂，加密和解密的速度比较慢，它的优点如下。

（1）公钥加密技术与对称加密技术相比，其优势在于不需要共享通用的密钥。

（2）公钥在传递和发布过程中即使被截获，由于没有与公钥相匹配的私钥，截获的公钥对入侵者没有太大意义。

（3）密钥少，便于管理，*N* 个用户通信只需要 *N* 对密钥，网络中的每个用户只需要保存自己的解密密钥。

（4）密钥分配简单，加密密钥分发给用户，而解密密钥由用户自己保留。

（5）保证数据的真实性和完整性，可以利用非对称密码算法进行数字签名。

非对称密码的缺点是加解密速度慢、密钥尺寸大、发展历史较短，一般不用于长文件和大量数据的加解密，主要用于数字签名认证和实体之间的密钥交换。

4. 解释 AES 解密算法。

答：由于 AES 是对称密码算法，因此 AES 的解密算法是对加密算法的逆运算，具体如图 2-1 所示。

5. 编写程序，实现 AES 加密算法。

答：AES 的加密与解密流程如图 2-1 所示。

AES 是分组密钥，算法输入 128 位数据，密钥长度也是 128 位。用 *Nr* 表示对一个数据分组加密的轮数。每一轮都需要一个与输入分组具有相同长度的扩展密钥 Expandedkey(i) 的参与。由于外部输入的加密密钥 *K* 长度有限，所以在算法中要用一个密钥扩展程序（Key Expansion）把外部密钥 *K* 扩展成更长的比特串,以生成各轮的加密和解密密钥。

（1）圈变化。

AES 每一个圈变换都由以下三个层组成。

非线性层——进行 Subbyte 变换。

线性混合层——进行 ShiftRow 和 MixColumn 运算。

密钥加层——进行 AddRoundKey 运算。

① Subbyte 变换是作用在状态中每字节上的一种非线性字节转换，可以通过计算出的 *S* 盒进行映射。

```
Schange:
    ldi zh,$01;将指针指向 S 盒的首地址
    mov zl,r2; 将要查找的数据作为指针低地址
    ldtemp,z+; 取出这个对应的数据
    mov r2,temp; 交换数据完成查表
    …
    ret
```

② ShiftRow 是一字节换位。它将状态中的行按照不同的偏移量进行循环移位，而这个偏移量也是根据 *Nb* 的不同而选择的。

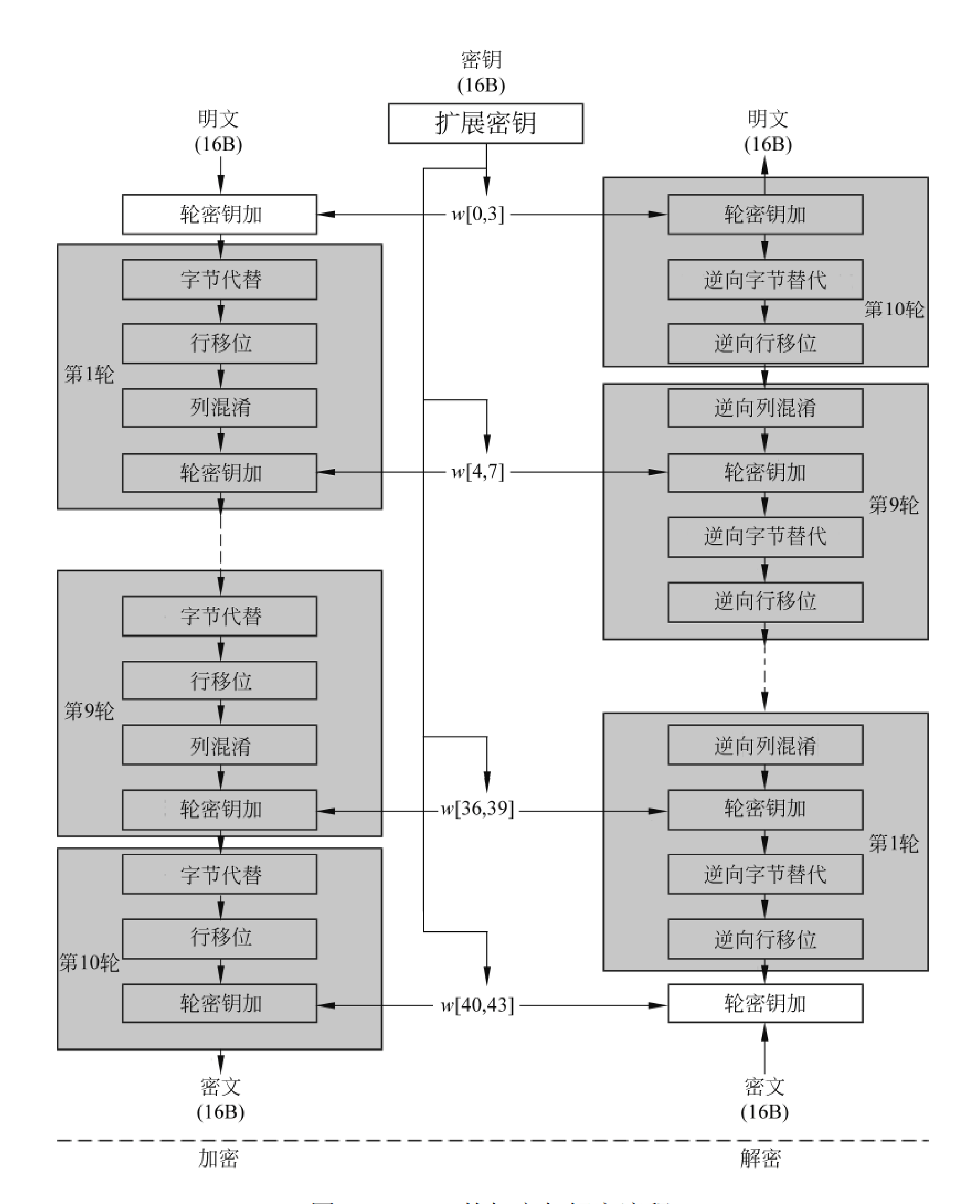


图 2-1　AES 的加密与解密流程

```
ShiftRow:;这是一字节换位的子程序
     mov temp,r3;因为是 4×4
     mov r3,r7; r2 r6 r10 r14 r2 r6 r10 r14
     mov r7,r11; r3 r7 r11 r15---r7 r11 r15 r3
     mov r11,r15; r4 r8 r12 r17 r12 r17 r4 r8
     mov r15,temp; r5 r9 r13 r18 r18 r5 r9 r13
     mov temp,r4
     mov temp1,r8
     mov r4,r12
     mov r8,r17
     mov r12,temp
     mov r17,temp1
     mov temp,r18
     mov r18,r13
     mov r13,r9
```

```
mov r9,r5
mov r5,temp
ret
```

③ 在 MixColumn 变换中把状态中的每一列看作 GF(28)上的多项式 $a(x)$与固定多项式 $c(x)$相乘的结果。$b(x)=c(x)*a(x)$的系数这样计算：*运算不是普通的乘法运算，而是特殊的运算，即

$b(x)=c(x)?a(x)(\mathrm{mod}\ x4+1)$

对于这个运算，

$b0=02\circ a0+03\circ a1+a2+a3$

令 xtime($a0$)=$02\circ a0$

其中，符号“。”表示模一个八次不可约多项式的同余乘法。

```
mov temp,a0;这是一个 MixColumn 子程序
rcall xtime;调用 xtime 程序
mov a0,temp
mov temp,a1
rcall xtime
eor a0,a1
eor a0,temp
eor a0,a2
…
xtime:;这是一个子程序
    ldi temp1,$1b
    lsl temp
    brcs next1;如果最高位是 1,则转移
next: ret;否则什么也不变化
   next1:eor temp,temp1
     rjmp next
```

对于逆变化，其矩阵 ***C*** 要改变成相应的 *D*，即 $b(x)=d(x)*a(x)$。

④ 密钥加层运算(addround)是将圈密钥状态中的对应字节按位“异或”。

⑤ 根据线性变化的性质，解密运算是加密变化的逆变化。这里不再详细叙述。

（2）轮变化。

（3）密钥扩展。

AES 算法利用外部输入密钥 *K*（密钥串的字数为 *Nk*），通过密钥的扩展程序得到共计 4(*Nr*+1)字的扩展密钥。它涉及如下 3 个模块。

① 位置变换(rotword)——把一个 4B 的序列[A,B,C,D]变换成[B,C,D,A]。

② *S* 盒变换(subword)——对一个 4B 进行 *S* 盒代替。

③ 变换 Rcon[i]——Rcon[i]表示 32 位比特字[xi-1,00,00,00]。这里的 x 是（02），如 Rcon[1]=[01000000]；Rcon[2]=[02000000]；Rcon[3]=[04000000]……

扩展密钥的生成：扩展密钥的前 *Nk* 个字就是外部密钥 *K*；以后的字 *W*[[*i*]]等于它前一个字 *W*[[*i*−1]]与前第 *Nk* 个字 *W*[[*i*−*Nk*]]的“异或”,即 *W*[[*i*]]=*W*[[*i*−1]] *W*[[*i*−*Nk*]]。但是，若 *i* 为 *Nk* 的倍数，则 *W*[*i*]=*W*[*i*−*Nk*] Subword(Rotword(*W*[[*i*−1]])) Rcon[*i*/*Nk*]。

程序执行的时候，主要调用以上几个子程序，具体实现如下。

```
Key Expansion:
    rcall rotword
    rcall subword
    rcall Rcon
    …
```

6. 具有 N 个节点的网络如果使用公开密钥密码算法，每个节点的密钥有多少？网络中的密钥共有多少？

答：N, $N+N(N+1)/2$。

7. 在非对称密码体制中，第三方如何断定通信者有无抵赖或伪造行为？

答：采用有仲裁的数字签名即可。

8. 设通信双方使用 RSA 加密体制，接收方的公开密钥是$(e,n)=(5,35)$，求明文 $M=30$ 对应的密文。

答：接收方的公开密钥是$(e,n)=(5,35)$，按照 RSA 算法知，$n=p*q=5*7$，所以 $p=5$，$q=7$，$\Phi(n) = (p-1)(q-1)= 4\times6=24$。

取 $e=5$，$1<e<\Phi(n)$，求出 d，使得 $ed\equiv1 \bmod 24$ 且小于 24。

因为 $5\times5=24+1$，所以 $d=5$。因此，公钥为$(e, n)=(5,35)$，私钥为$(d, n)=(5,35)$。

对于明文 $M=30$，加密后为

$C=M^e \bmod n=30^5 \bmod 35=24300000 \bmod 35 = 3300000 \bmod 35=25$

所以，明文 $M=30$ 对应的密文 $C=25$。

9. 在使用 RSA 公钥的通信中，若截取了发送给其他用户的密文 $C=10$，并且用户的公钥为$(e, n)=(5, 35)$，求对应的明文。

答：如果 $C=10$，明文 $M=C^d \bmod n=10^5 \bmod 35 = 100000 \bmod 35 = 5$，即对应的明文为 5。

10. 什么是序列密码和分组密码？

答：序列密码也称流密码，是从随机数序列的产生中得到启发的，如果每次对一个密钥流发生器输入不同的种子密钥，就会生成不同的密钥序列。这是一种对称加密技术。

分组密码是将明文消息编码表示后的数字（简称明文数字）序列划分成长度为 n 的组（可看成长度为 n 的矢量），每组分别在密钥的控制下变换成等长的输出数字（简称密文数字）序列。采用分组编码的好处是易于标准化。

11. 简述通信双方如何使用密钥体制建立通信中的信任关系。

答：采用密钥分配中心连接用户间的密钥和用户之间直接传递密钥两种方法。

12. 有哪些建立公开密钥体制的方法？

答：KDC（密钥分配中心）和数字证书。

13. 常规加密密钥的分配有几种方案，请对比它们的优缺点。

答：在密钥管理中，最关键的问题就是密钥分配——主要涉及密钥的发送和验收，密钥的发送需要非常安全的通道，密钥的验收需要检验密钥发送的正确性。

密钥的分配有两种方案：网内分配和网外分配。网外分配指派非常可靠的信使，如邮递员或信鸽等携带密钥分配给各用户。但是，如果用户数过大，黑客技术的发展使得密钥使用量增大，且要求频繁更换，则网外分配不可行，这时需要采用网内分配，即自动密钥分配。

网内分配又分两种形式：用户之间直接分配和通过密钥中心分配。

14. 如何利用公开密钥加密进行单钥加密密钥的分配？

答：对于通信双方来说，若需要进行密钥的分配，则 A 发送给 B 经过 B 公钥加密的密钥，B 利用私钥解密。可以采用非对称加密算法（如 RSA）完成。

15. 什么是无碰撞单向哈希函数？

答：哈希函数 H 把一个值 x（值 x 属于一个有很多个值的集合（或者是无穷多个值））影射到另外一个值 y，y 属于一个有固定数量个值（少于前面集合）的集合。如果一个哈希函数 H 具有单向函数的性质——也就是：给定一个值 x，很容易计算 $H(x)$，但是，给定一个值 y，很难找到一个值 x，使得 $H(x)=y$，这个哈希函数 H 叫作单向哈希函数。如果对于此 H 函数不同的输入值不可能产生相同的输出值，就称此 H 函数为无碰撞单向哈希函数。

16. 单钥加密体制的密钥分配有哪几种方法？它们分别有什么优缺点？

答：单钥加密体制也称对称加密体制，它对于用户 A、B 的密钥分配有四种方法。

① 由 A 发送给 B。

② 由第三方发送给 A 和 B。

这两种方法称为人工发送，如果有 n 个用户，则密钥数目为 $n(n-1)/2$。n 很大时，人工发送是不可行的。

③ 已有的共享密钥加密新密钥并发送给另一方。

这种方法的缺点是攻击者一旦获得一个密钥，就可获取以后所有的密钥，用这种方法对所有用户分配初始密钥时，代价仍然很大。

④ 第三方 C 为 A、B 选取密钥后，分别在两个保密信道上发送给 A、B。

这种方法比较常用，其中的第三方通常是一个负责为用户分配密钥的密钥分配中心。

这时每一用户必须和密钥分配中心有一个共享密钥（称为主密钥）。通过主密钥分配给一对用户的密钥称为会话密钥，用于这一对用户之间的保密通信。通信完成后，会话密钥即被销毁。

17. 假定两个用户 A、B 分别与密钥分配中心（key distribution center，KDC）有一个共享的主密钥 K_A 和 K_B（图 2-2），A 希望与 B 建立一个共享的一次性会话密钥，需要完成哪些步骤？

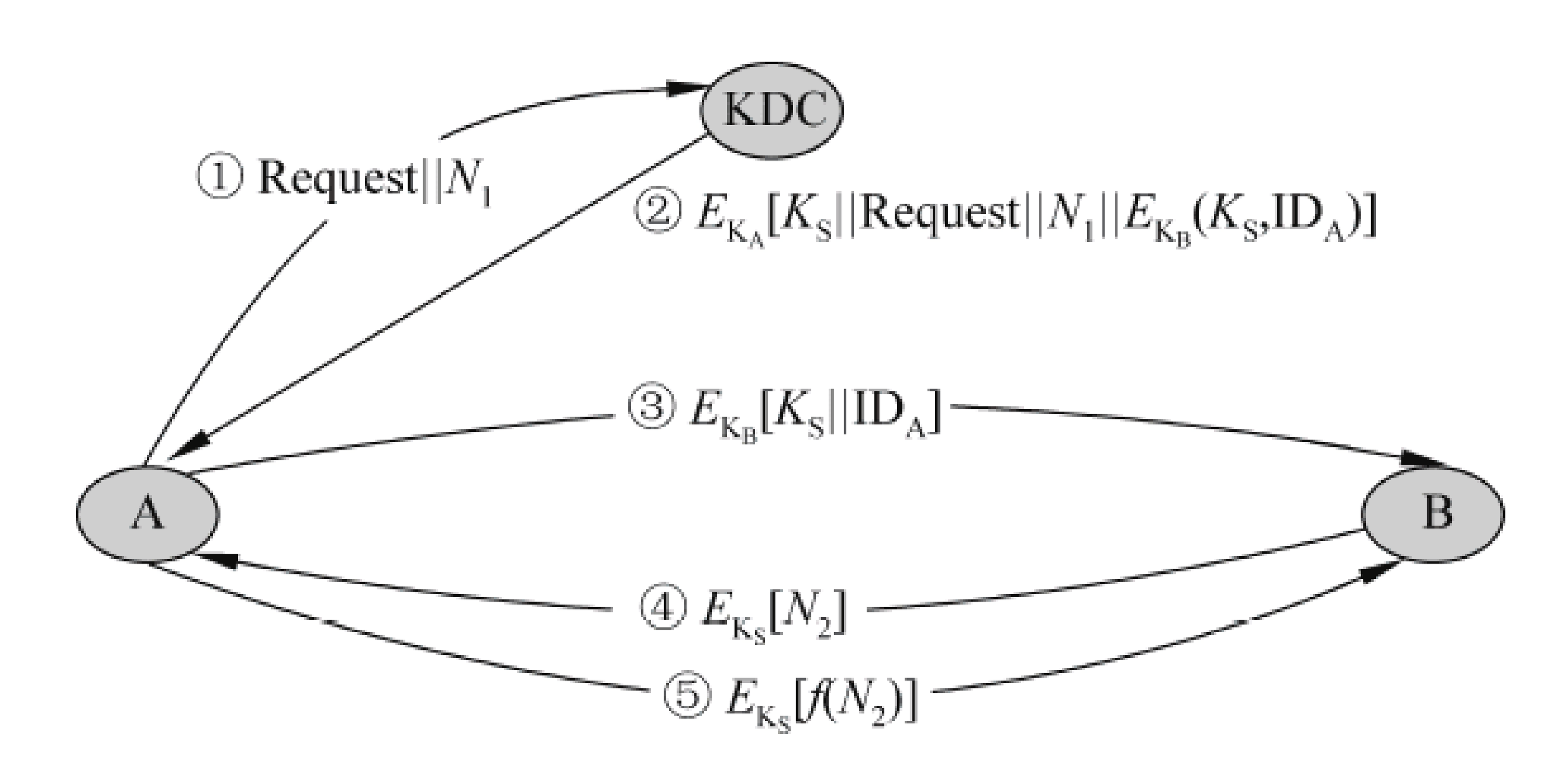


图 2-2　密钥分配中心 KDC 为 A 与 B 建立一个共享的一次性会话密钥过程

答：① A 向 KDC 发出会话密钥请求。表示请求的消息由两个数据项组成，第 1 项是 A 的身份，第 2 项是这次业务的唯一识别符 N_1，称 N_1 为一次性随机数，可以是时间戳、计数器或随机数。每次请求用的 N_1 都应不同，且为防止假冒，应使敌手对 N_1 难以猜测，因此用随机数作这个识别符最合适。

② KDC 为 A 的请求发出应答。应答是由 K_A 加密的消息，因此只有 A 才能成功地对这一消息解密，并且 A 可相信这一消息的确是由 KDC 发出的。消息中包括 A 希望得到的两项内容：

i．一次性会话密钥 K_S。

ii．A 在①中发出的请求，包括一次性随机数 N_1，目的是使 A 将收到的应答与发出的请求相比较，看是否匹配。

因此，A 能验证自己发出的请求在被 KDC 收到之前是否被他人篡改，而且 A 还能根据一次性随机数相信自己收到的应答不是重放的过去的应答。此外，消息中还有 B 希望得到的两项内容：

i．一次性会话密钥 K_S。

ii．A 的身份（如 A 的网络地址）ID_A。

这两项由 K_B 加密，将由 A 转发给 B，以建立 A、B 之间的连接并用于向 B 证明 A 的身份。

③ A 存储会话密钥，并向 B 转发 $EK_B[K_S \| \text{ID}_A]$。因为转发的是由 K_B 加密后的密文，所以转发过程不会被窃听。B 收到后，可得会话密钥 K_S，并从 ID_A 可知另一方是 A，而且还从 EK_B 知道 K_S 的确来自 KDC。

这一步完成后，会话密钥就安全地分配给了 A、B。然而，还能继续以下两步工作：

④ B 用会话密钥 K_S 加密另一个一次性随机数 N_2，并将加密结果发送给 A。

⑤ A 以 $f(N_2)$作为对 B 的应答，其中 f 是对 N_2 进行某种变换（例如，加 1）的函数，并将应答用会话密钥加密后发送给 B。这两步可使 B 相信第③步收到的消息不是一个重放。

18. 什么是密钥的分层控制？这种方法有什么优点？

答：把一个大范围划分成许多小范围，在每个小范围（如一个 LAN 或一个建筑物）内都建立一个本地密钥分配中心 KDC。同一范围的用户在进行保密通信时，由本地 KDC 为他们分配密钥。如果两个不同范围的用户想获得共享密钥，则可通过各自的本地 KDC，而两个本地 KDC 的沟通又须经过一个全局 KDC，这样就建立了两层 KDC。类似地，根据网络中用户的数目及分布的地域，可建立 3 层或多层 KDC。这种方法的优点是：

（1）可减少主密钥的分布，因为大多数主密钥是在本地 KDC 和本地用户之间共享的。

（2）分层结构还可将虚假 KDC 的危害限制到一个局部区域。

19. 无中心的密钥分配时，两个用户 A 和 B 建立会话密钥须经过哪几步？

答：无中心的密钥分配时，两个用户 A 和 B 建立会话密钥须经过以下 3 步，如图 2-3 所示。

① A 向 B 发出建立会话密钥的请求和一个一次性随机数 N_1。

② B 用与 A 共享的主密钥 MK_m 对应答的消息加密，并发送给 A。应答的消息中有 B 选取的会话密钥、B 的身份、$f(N_1)$和另一个一次性随机数 N_2。

③ A 使用新建立的会话密钥 K_S 对 $f(N_2)$加密后返回给 B。

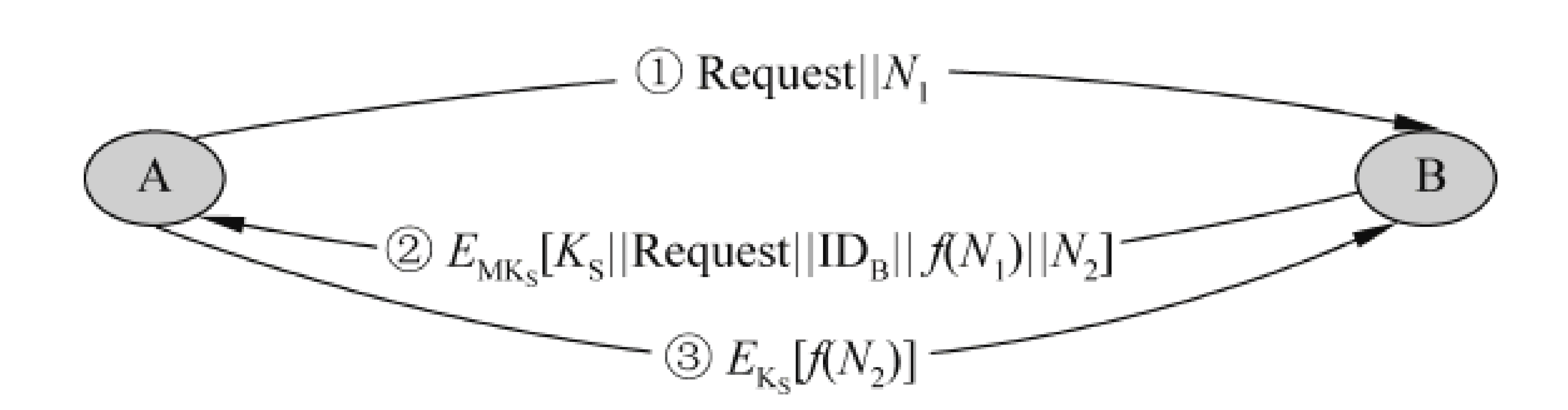


图 2-3　无中心时 A 与 B 建立一个共享的一次性会话密钥过程

20. 单钥体制中的密钥控制技术是什么？

答：密钥标签和控制矢量。

21. 公钥管理机构向用户 A、B 分配公钥共有哪几步？

答：公钥管理机构向用户 A、B 分配公钥如图 2-4 所示。

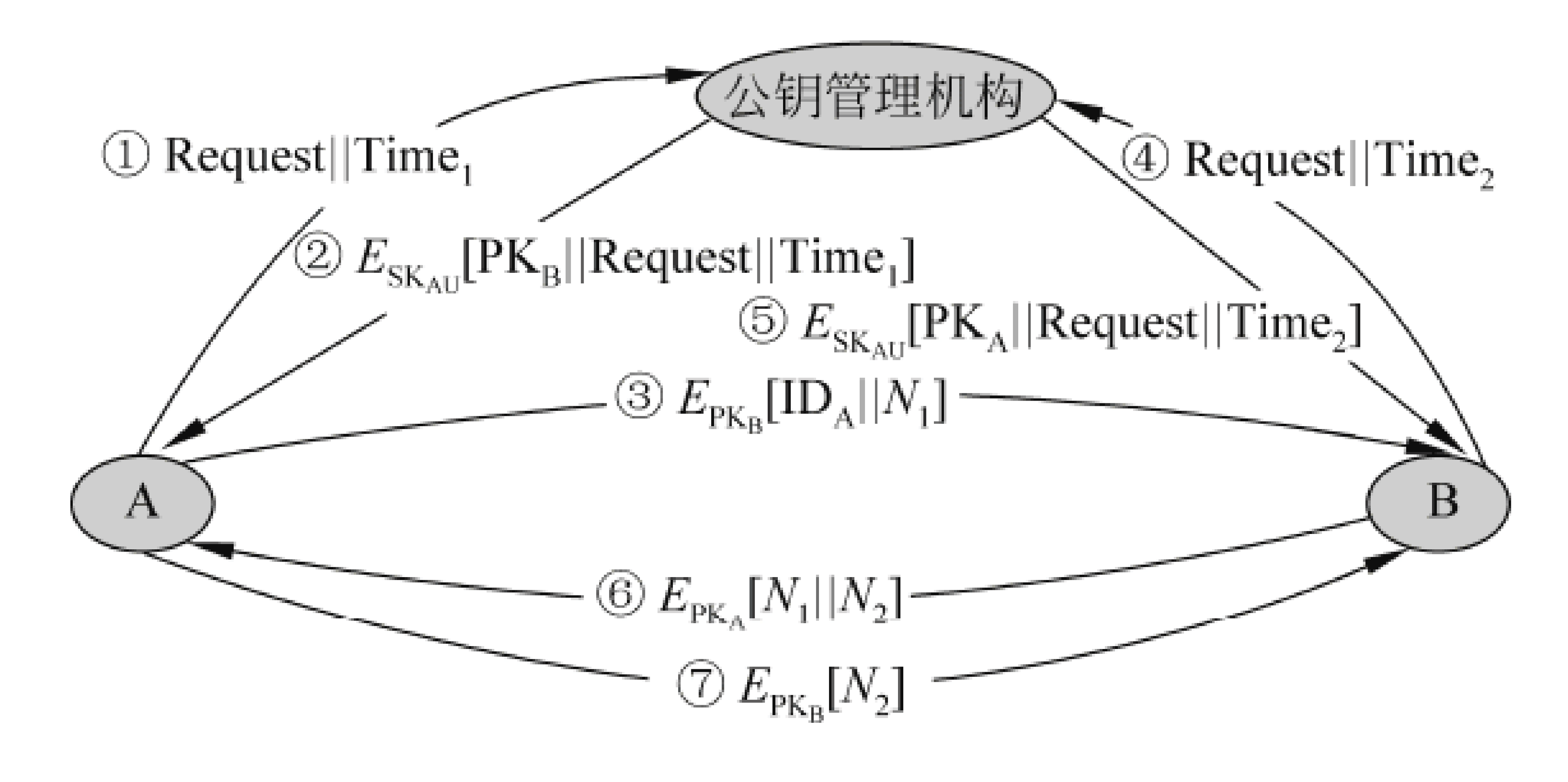


图 2-4　公钥管理机构向用户 A、B 分配公钥

① 用户 A 向公钥管理机构发送一个带时间戳的消息，消息中有获取用户 B 的当前公钥的请求。

② 管理机构对 A 的请求做出应答，应答由一个消息表示，该消息由管理机构用自己的密钥 SKAU 加密，因此 A 能用管理机构的公开钥解密，并使 A 相信这个消息的确来源于管理机构。

应答的消息中有以下三项。

a. B 的公钥 PK_B，A 可用之对将发往 B 的消息加密。

b. A 的请求，用于 A 验证收到的应答的确是对相应请求的应答，且还能验证自己最初发出的请求在被管理机构收到以前是否被篡改。

c. 最初的时间戳，以使 A 相信管理机构发来的消息不是一个旧消息，因此消息中的公开钥的确是 B 当前的公钥。

③ A 用 B 的公开钥对一个消息加密后发往 B，这个消息有两个数据项：一是 A 的身份 ID_A，二是一个一次性随机数 N_1，用于唯一地标识这次业务。

④⑤ B 以相同的方式从管理机构获取 A 的公开钥（与步骤①、②类似）。这时，A 和 B 都已安全地得到了对方的公钥，所以可进行保密通信。然而，他们也许还希望有以下两步，以认证对方。

⑥ B 用 PK_A 对一个消息加密后发往 A，该消息的数据项有 A 的一次性随机数 N_1 和 B 产生的一个一次性随机数 N_2。因为，只有 B 能解密③的消息，所以 A 收到的消息中的 N_1 可使其相信通信的另一方的确是 B。

⑦ A 用 B 的公开钥对 N_2 加密后返回给 B，可使 B 相信通信的另一方的确是 A。

22. 请自己设计一个密钥生成算法，并验证其密钥空间的安全性。

答：略

23. 在密钥的生存期间内，如何对密钥进行有效的管理？

答：密钥的管理包括密钥的分配、控制使用、保护和存储。

密钥分配涉及密钥的发送和验收。前者要求通过非常安全的通路进行传送，后者要求有一套机制用于检验分发和传送的正确性。网内密钥分配的方式有两种：用户之间直接分配以及通过设立一个密钥分配中心（Key Distribution Center，KDC）分配。

密钥的控制使用是为了保证密钥按照预定的方式使用，控制密钥使用的信息有以下几项：密钥主权人；密钥合法使用期限；密钥标识符；密钥预定用途；密钥预定算法；密钥预定使用系统；密钥授权用户和密钥生成、注册、证书等有关实体中的名字等。

密钥的保护和存储包括密钥从产生到终结，在整个生存期的保护，一些基本措施如下。密钥绝不能以明文形式存放；密钥首先选择物理上最安全的地方存放；在有些系统中可以使用密钥碾碎技术由一个短语生成单密钥；可以将密钥分开存放。例如，将密钥平分成两段，一段存入终端，一段存入 ROM；或者将密钥分成若干片，分给不同的可信者保管。

24. 销毁被撤销的密钥时应注意什么？

答：密钥被替换后，旧密钥必须被销毁。旧密钥虽然不再使用，却可以给攻击者提供许多有重大参考价值的信息，为攻击者推测新的密钥提供许多有价值的信息。为此，必须

保证被销毁的密钥不能给任何人提供丝毫有价值的信息。下面是一些常用的方法。

（1）密钥写在纸上时，要把纸张粉碎或烧毁。

（2）密钥写在 EEPROM 中时，要对 EEPROM 进行多次重写。

（3）密钥存在 EPROM 或 PROM 中时，应将 EPROM 或 PROM 打碎成小片。

（4）密钥存在磁盘中时，应当多次重写覆盖密钥的存储位置，或将磁盘切碎。

（5）要特别注意对存放在多个地方的密钥的同时销毁。

25. KDC 在密钥分配过程中充当什么角色？

答：（1）在对称密码体制下，是 A、B 双方共同信任的第三方，负责分发单密钥。

（2）在非对称密码体制下，管理 A、B 双方的私钥。

26. 简述信息隐藏的基本嵌入和检测过程。

答：信息隐藏的起源可以追溯到古代的隐写术，这是一种将秘密信息以不可见的形式隐藏于非秘密的公开数据中，而在数据传输与存储的过程中不被外界察觉，当合法接收者获得含密公开数据后，按照已约定的规则还原原始秘密信息的数据保护技术。这就如同给秘密信息涂上了一层保护色，巧妙地将自己隐藏起来，免于被攻击者发现导致遭受泄密与破坏。在信息技术高度发达的今天，数字信息与隐写术相结合，使数字信息隐藏成为一门全新的技术。

实施信息隐藏的基本流程如图 2-5 所示，秘密信息通过特定的密钥与嵌入算法的结合隐藏到载体数据中形成含密数据，而当需要获取秘密信息时，通过特定密钥和提取算法对含密数据进行秘密信息的提取，从而得到秘密信息。

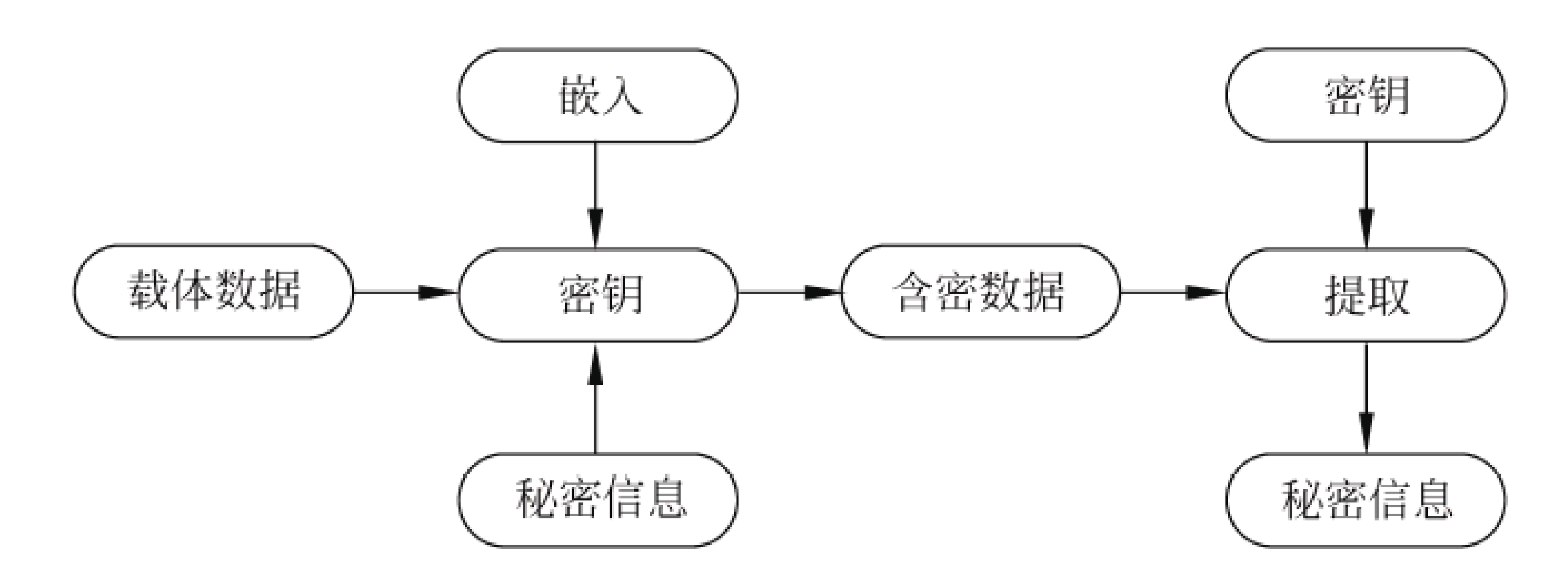


图 2-5　实施信息隐藏的基本流程

27. 简述数字水印的定义和内容。

答：数字水印（digital watermarking）指把一些标识信息（即数字水印）直接嵌入数字载体中（包括多媒体、文档、软件等）或是间接表示（修改特定区域的结构），且不影响原载体的使用价值，也不容易被探知和再次修改。数字水印可以被生产方识别和辨认，通过隐藏在载体中的信息，可以达到确认内容创建者、购买者、传送隐秘信息或者判断载体是否被篡改等目的。数字水印是保护信息安全、实现防伪溯源、版权保护的有效办法，是信息隐藏技术研究领域的重要分支和研究方向。

数字水印技术是从信息隐藏技术发展而来的，是数字信号处理、图像处理、密码学应用、算法设计等学科的交叉领域。数字水印最早在 1993 年由 Tirkel 等人提出，在国际学术

会议上发表题为 *Electronic Watermark* 的第一篇有关水印的文章，提出了数字水印的概念及可能的应用，并针对灰度图像提出了两种向图像最低有效位中嵌入水印的算法。1996 年，在英国剑桥牛顿研究所召开了第一届国际信息隐藏学术研讨会，标志着信息隐藏学的诞生。

数字水印技术基本上具有下面四个方面的特点。

（1）安全性：数字水印的信息应是安全的，难以篡改或伪造，同时，应当有较低的误检测率，当原内容发生变化时，数字水印应当发生变化，从而可以检测原始数据的变更；当然，数字水印同样对重复添加有很强的抵抗性。

（2）隐蔽性：数字水印应是不可知觉的，而且应不影响被保护数据的正常使用；不会降质。

（3）鲁棒性：是指在经历多种无意或有意的信号处理过程后，数字水印仍能保持部分完整性并能被准确鉴别。可能的信号处理过程包括信道噪声、滤波、数/模与模/数转换、重采样、剪切、位移、尺度变化以及有损压缩编码等。

（4）嵌入容量（embedding capacity）：是指载体在不发生形变的前提下可嵌入的水印信息量，尤其是隐蔽通信领域的特殊性，对水印的容量需求很大。

水印算法是将信息嵌入到随机选择的图像点中最不重要的像素位（least significant bits，LSB）上，这可保证嵌入的水印是不可见的。但是，由于使用了图像不重要的像素位，算法的鲁棒性差，水印信息很容易被滤波、图像量化、几何变形的操作破坏。另外一个常用的方法是利用像素的统计特征将信息嵌入像素的亮度值中。

大部分水印算法都采用了扩展频谱通信（spread spectrum communication）技术。算法实现过程为：先计算图像的离散余弦变换（DCT），然后将水印叠加到 DCT 域中幅值最大的前 k 系数上（不包括直流分量），通常为图像的低频分量。若 DCT 系数的前 k 个最大分量表示为 $D=i$，$i=1$，2，…，k，水印是服从高斯分布的随机实数序列 $W = i$，$i=1$，2，…，k，那么水印的嵌入算法为 $di = di(1 + awi)$，其中常数 a 为尺度因子，控制水印添加的强度。然后用新的系数作反变换得到水印图像 I。解码函数则分别计算原始图像 I 和水印图像 I*的离散余弦变换，并提取嵌入的水印 W*，再做相关检验，以确定水印是否存在。该方法即使当水印图像经过一些通用的几何变形和信号处理操作而产生比较明显的变形后，仍然能够提取出一个可信赖的水印副本。一个简单的改进是不将水印嵌入到 DCT 域的低频分量上，而是嵌入到中频分量上，以调节水印的顽健性与不可见性之间的矛盾。另外，还可以将数字图像的空间域数据通过离散傅里叶变换（DFT）或离散小波变换（DWT）转换为相应的频域系数；其次，根据待隐藏的信息类型，对其进行适当编码或变形；再次，根据隐藏信息量的大小和其相应的安全目标选择某些类型的频域系数序列（如高频或中频，或低频）；再次，确定某种规则或算法，用待隐藏的信息的相应数据修改前面选定的频域系数序列；最后，将数字图像的频域系数经相应的反变换转换为空间域数据。该类算法的隐藏和提取信息操作复杂，隐藏信息量不能很大，但抗攻击能力强，很适合数字作品版权保护的数字水印技术。

28. 简述数字隐藏技术中隐含的信任关系。

答：每个用户间不直接建立信任关系，而是通过上层数字中心与中心之间建立信任关系。

29. 收集国内外有关加密或信息隐藏技术的最新动态。

答：信息隐藏是指在设计和确定模块时，使得一个模块内包含的特定信息（过程或数据）对于不需要这些信息的其他模块来说是不可访问的。

30. 分析消息认证码可能遭受的攻击。

答：消息认证码保证了传输数据的完整性，但却不能保证真实性。对于通信双方 A 和 B，B 可以通过伪造 MAC 地址，或者宣称收到由 A 发来的消息，实际是伪造的消息来实施诈骗等非授权行为。

31. 数字签名有什么作用？

答：数字签名的作用是确认数据单元来源和数据单元的完整性，并保护数据，防止被人进行伪造。

32. 描述报文鉴别码和杂凑码的区别。

答：杂凑码也称哈希码，是通过哈希函数将一个任意长度的消息压缩到一个固定长度的码，这个码就称为哈希码。

报文鉴别码是指鉴别数据的一个码，它的作用是防篡改和保密数据，它可以是杂凑码，也可以是由其他算法产生的码。

33. 简述数字签名的用途和基本流程。

答：在日常生活中，为了确认一件作品及其出处，常采用签名、骑缝、盖章等手段，以便于鉴别。在数字通信中也需要做同样的工作。

在数字通信中，也会发生一方对另一方的欺骗行为，如否认：发送方否认自己发送过某个报文，或接收方接收某个报文后否认接收过。

34. 什么是数字签名？什么是消息认证？

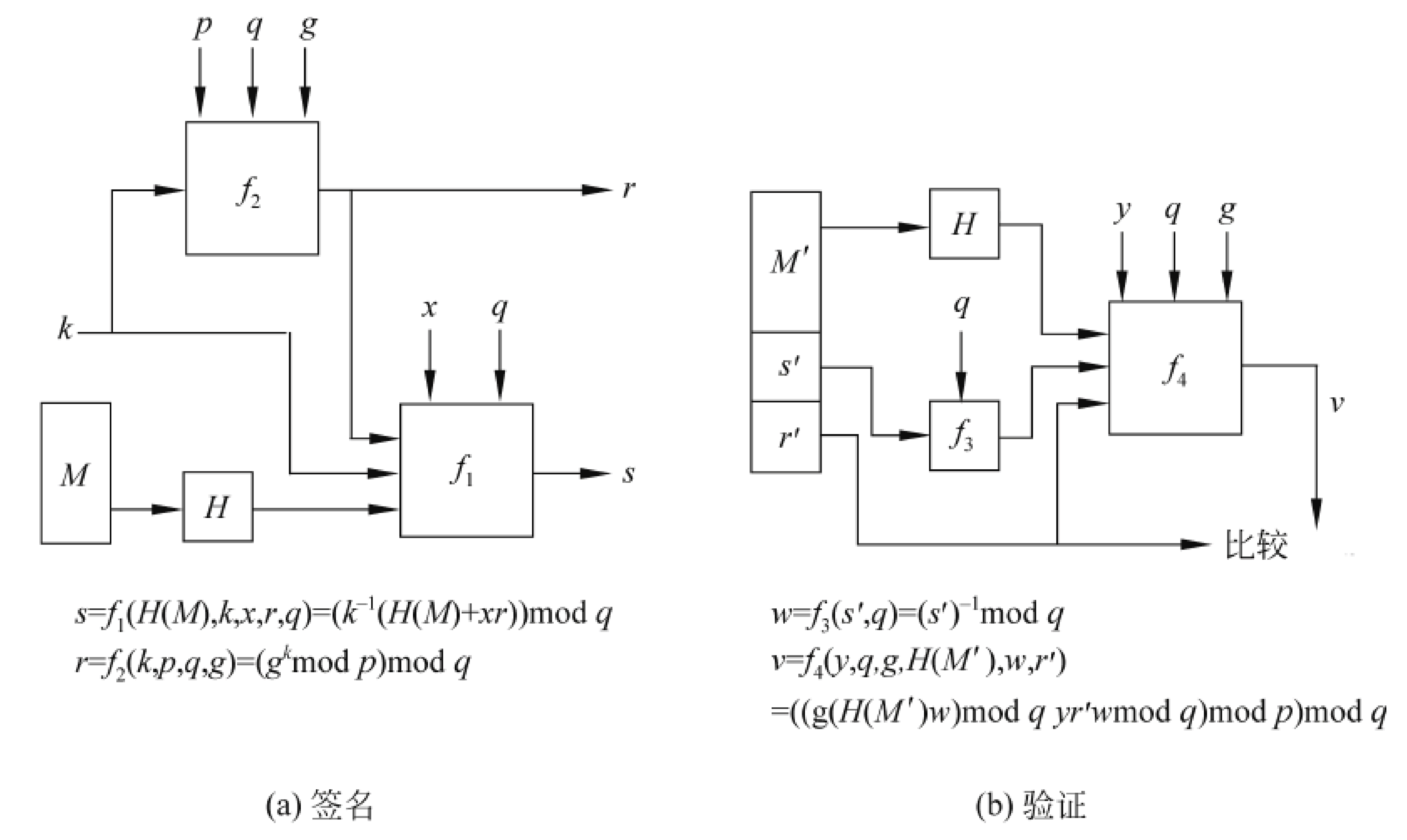
答：在 ISO 7498-2 标准中，数字签名定义为：附加在数据单元上的一些数据，或是对数据单元所做的密码变换，这种数据和变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性，并保护数据，防止被恶意进行伪造。

消息认证也称报文鉴别，是检测传输和存储的消息（报文）有无受到完整性攻击的手段，它包括了消息内容认证（即消息完整性认证）、消息的序列认证和操作时间认证等。其核心是消息（报文）的内容认证。

35. 美国数字签名标准（Digital Signature Standard，DSS）方案（图 2-6）的具体内容是

什么？

答：



(a) 签名　　(b) 验证

图 2-6　美国数字签名标准方案

美国数字签名标准方案如图 2-6 所示。

（1）DSS 算法参数说明。

DSS 算法中应用了下述参数：

p：L bits 长的素数。L 是 64 的倍数，范围是 512～1024。

q：$p-1$ 的 160bits 的素因子。

g：$g = h(p-1)/q \bmod p$，h 满足 $h < p-1$, $h(p-1)/q \bmod p > 1$。

x：$1<x<q$，x 为私钥。

y：$y = gx \bmod p$，(p, q, g, y)为公钥。

$H(x)$：单向 Hash 函数。在 DSS 中选用安全散列算法（secure hash algorithm，SHA）。

p, q, g：可由一组用户共享，但在实际应用中，使用公共模数可能会带来一定的威胁。

（2）签名及验证协议。

签名及验证协议如下：

① P 产生随机数 k，$k < q$。

② P 计算 $r = (gk \bmod p) \bmod q$ 和 $s = (k-1\ (H(M) + xr)) \bmod q$。

M 是消息，签名结果是(M, r, s)。

③ 验证时，假设收到的信息为(M', r', s')

计算 $w = s' - 1 \bmod q$

计算 $u1 = (H(M') \times w) \bmod q$

计算 $u2 = (r' \times w) \bmod q$

计算 $v = ((gu1 * yu2) \bmod p) \bmod q$

若 $v = r'$，则认为签名有效。

36. 要将明文 M 由 $A1$ 并附有 $A1$、$A2$、…、Ai、…、An 的依次签名发往 B。设 PKAi 和 SKAi 分别为 Ai 的公开密钥和私有密钥，在签名时要求每一位签名者只验证其前一位签名者的签名；如果验证通过，则在此基础上加上自己的签名，否则终止签名；最后一位签名者在签名完成后将最终信息和签名一起发送出去。每一位签名者都可以推算出前一位签名者和后一位签名者并且知道他们的公开密钥。试设计该多人签名算法。

答：略

37. 查阅相关资料，比较各种数字签名算法的优缺点。

答：数字签名算法有 RSA、椭圆曲线等公钥密码（ECC）算法。

RSA 数字签名的算法优点是简单、实用、强度高、不易被破解，其缺点是慢、密钥太大、每次加密块比较小。

椭圆曲线公钥系统（ECC）是代替 RSA 的强有力的竞争者。椭圆曲线数字签名与 RSA 方法相比，有以下优点：

（1）安全性能更高。如 160 位 ECC 与 1024 位 RSA 有相同的安全强度。

（2）计算量小，处理速度快。在私钥的处理速度上（解密和签名），ECC 远比 RSA、DSA 快得多。

（3）存储空间占用小。ECC 的密钥尺寸和系统参数与 RSA、DSA 相比要小得多，所以占用的存储空间小得多。

（4）带宽要求低使得 ECC 具有广泛的应用前景。

38. 可信第三方有什么作用？

答：仲裁判决。

39. 简述一个成功的 SET 交易的标准流程。

答：SET 是 Secure Electric Transaction 的缩写，指安全电子交易。一个成功的 SET 标准流程为：①订货，消费者上网，查看商品并提交给商家；②支付，商家核对订货单，向用户发出支付通知，向银行发出转账请求；③转账，发卡机构验证消费者的支付卡后，将卡号加密传向支付网关，银行审查消费者支付卡合格后进行转账，转账成功后，支付网关向商家和发卡机构发出转账成功回执，发卡机构向消费者发出支付收据；④付货，商家向消费者付货。

40. 电子支付中有哪些安全需求?

答：一是交易双方信息和交易环境的安全需求；二是如何保证交易的真实可靠性，包括可能存在的窃听、篡改交易者个人及资金信息等。

41. SET（安全电子交易）中有哪些关键技术？

答：数字信封、数字签名、双重签名等。

第 3 章　身份认证与访问控制

3.1　第 3 章知识提要

本章主要介绍了身份认证和数字签名，基于生物特征、静态口令、动态口令、密钥分发、数字证书的身份认证，以及采用非对称密码体制的数字签名。为了保证消息的完整性，还需要采用消息认证或报文摘要法。常见的国际数字证书标准 X.509 以及以公开密钥加密法为中心的密钥管理体系结构 PKI、Kerberos 体制的数字认证，为了对合法用户进行权限划分，还介绍了自主、强制、基于角色的访问控制策略。从访问者的角度把系统分为主体和客体两部分，涉及访问控制矩阵、授权关系表、访问能力表、访问控制表等形式。

3.2　第 3 章习题和答案详解

一、选择题（答案：BBCCA DADBA DACB）

1. 用数字办法确认、鉴定、认证网络上参与信息交流者或服务器的身份是指________。
   A. 接入控制
   B. 数字认证
   C. 数字签名
   D. 防火墙

答案：B

解答：只有B的定义与题中的描述相符。

2. 身份鉴别是安全服务中的重要一环，以下关于身份鉴别的叙述中，不正确的是________。
   A. 身份鉴别是授权控制的基础
   B. 身份鉴别一般不用提供双向的认证
   C. 目前一般采用基于对称密钥加密或公开密钥加密的方法
   D. 数字签名机制是实现身份鉴别的重要机制

答案：B

解答：身份鉴别包括采用双向认证的方法，因此选择B。

3. 以下关于CA认证中心说法正确的是________。
   A. CA认证是使用对称密钥机制的认证方法
   B. CA认证中心只负责签名，不负责证书的产生
   C. CA认证中心负责证书的颁发和管理，并依靠证书证明一个用户的身份

D. CA认证中心不用保持中立，可以随便找一个用户作为CA认证中心

答案：C

解答：CA（认证中心）负责证书的颁发和管理，并依靠证书证明一个用户的身份。

4. Kerberos的设计目标不包括________。

A. 认证

B. 授权

C. 记账

D. 审计

答案：C

解答：Kerberos的设计目标不包括记账。

5. 访问控制是指确定________以及实施访问权限的过程。

A. 用户权限

B. 可给予哪些主体访问权利

C. 可被用户访问的资源

D. 系统是否遭受入侵

答案：A

解答：访问控制是指确定用户权限以及实施访问权限的过程。

6. 下列对访问控制影响不大的是________。

A. 主体身份

B. 客体身份

C. 访问类型

D. 主体与客体的类型

答案：D

解答：对访问控制影响不大的是主体与客体的类型。

7. 为了简化管理，通常对访问者________，以避免访问控制表过于庞大。

A. 分类组织成组

B. 严格限制数量

C. 按访问时间排序，删除长期没有访问的用户

D. 不作任何限制

答案：A

解答：为了简化管理，通常对访问者分类组织成组，以避免访问控制表过于庞大。

8. PKI支持的服务不包括________。

A. 非对称密钥技术及证书管理

B. 目录服务
C. 对称密钥的产生和分发
D. 访问控制服务

答案：D

解答：PKI服务不包括访问控制。

9. PKI的主要组成不包括________。
A. 证书授权CA
B. SSL
C. 注册授权RA
D. 证书存储库CR

答案：B

解答：PKI的主要组成不包括SSL。

10. PKI管理对象不包括________。
A. ID和口令
B. 证书
C. 密钥
D. 证书撤销

答案：A

解答：PKI管理对象不包括ID和口令。

11. 下面不属于PKI组成部分的是________。
A. 证书主体
B. 使用证书的应用和系统
C. 证书权威机构
D. AS

答案：D

解答：PKI的组成部分包括政策批准结构（Policy Acception Authority，PAA），政策认证机构（Policy Certification Authority，PCA），认证机构（Certification Authority，CA），在线注册机构（Online Registration Authority，ORA），不包括AS。

12. PKI能够执行的功能是________和________。
A. 鉴别计算机消息的始发者
B. 确认计算机的物理位置
C. 保守消息的机密
D. 确认用户具有的安全性特权

答案：AC

解答：PKI能够执行的功能是鉴别计算机消息的始发者和保守消息的机密。

13. PKI的主要理论基础是________。

A. 对称密码算法

B. 公钥密码算法

C. 量子密码

D. 摘要算法

答案：B

解答：PKI的主要理论基础是公钥密码算法。

二、填空题

答案：1. 身份认证，信源，信宿

2. 访问控制，访问权限

3. 数字证书，认证中心

1. 身份认证是验证信息发送者是真的，而不是冒充的，包括信源、信宿等的认证和识别。
2. 访问控制的目的是为了限制访问主体对访问客体的访问权限。
3. 数字证书是PKI的核心元素， 认证中心是PKI的核心执行者。

三、问答题

1. 简述生物特征身份认证的发展趋势。

答：提高生物特征识别的精确性和可靠性是未来的发展趋势。

2. 简述口令可能会遭受哪些攻击。

答：攻击口令的方式多种多样，常见的有以下 4 种。

（1）社会工程学。

（2）暴力破解。

（3）弱口令扫描。

（4）密码监听。

3. 假定只允许使用 26 个字母构造口令，在下列情况下各可以构造出多少条口令？

（1）口令最多可以使用 n 个字符，$n=4$，6，8，不区分大小写。

（2）口令最多可以使用 n 个字符，$n=4$，6，8，区分大小写。

答：（1）分别是 26 的 4 次方，26 的 6 次方，26 的 8 次方。

（2）分别是 52 的 4 次方，52 的 6 次方，52 的 8 次方。

4. 编写一个口令生成程序。程序以长度 s（可以取 s=8，16，32，64）的随机二进制种子作为输入。

（1）让多名用户使用你的程序生成口令，记录有多少人选择了相同的事件。

（2）生成一个口令并加密，然后让人通过尝试随机数种子的所有值进行口令攻击。事先要给定一个猜测次数的期望值。

答：略

5. 略

6. 比较动态口令的 3 种实现方式。

答：短信密码、软件令牌、硬件令牌。短信密码是通过手机短信形式发送 6 位或更多随机数的动态口令。软件令牌是通过软件生成随机密码。硬件令牌每 60s 变换一次动态口令。

7. 比较静态口令与动态口令。

答：静态口令不随时间变化，动态口令随时间而变化。

8. 常用动态令牌有哪几种？

答：（1）短信密码。

（2）手机令牌。

（3）硬件令牌。

（4）软件令牌。

9. 在身份验证中，可能会遇到重放攻击。重放具有如下几种形式：

（1）简单的重放：攻击者简单地复制信息，经过一段时间后，再重放原来的信息。

（2）重放不能被检测到：这时，原始的信息不能到达，只有重放信息到达目的地。

（3）没有定义的重放返回：发送者这时很难确定是发送信息，还是接收信息。

如何确定信息是否是重放的信息？

答：重放（replay）攻击是指在消息没有时间戳的情况下，攻击者利用身份认证机制中的漏洞先把别人有用的消息记录下来，过一段时间后再发送出去。

如果在发送信息中加上时间戳，就可以有效检测信息是否是重放信息。

10. 如何保护 IC 卡的安全？

答：对于 IC 卡，常用的攻击行为有以下 3 种。

（1）截取信道中的信息：通过非法设备以及相关技术手段读取 IC 卡中存储的数据信息以及在 IC 卡与读卡器进行操作时截取数据交换信息。

（2）破译 IC 卡中的信息：攻击者采用上述两种方式截获数据信息后，根据 IC 卡中数据信息的变化情况以及数据交换过程中数据流的变化对数据进行分析，从而确认 IC 卡中所有数据的含义以及数据流的变化规则，完成对 IC 卡中数据信息的破译，进而达到非法改变数据信息的目的。

（3）复制 IC 卡中的数据信息：攻击者在截获数据信息后，并不对数据进行分析破译，而是记录在特定操作中数据流的变化情况，在需要时将记录的数据流直接复制发送到 IC 卡，从而达到非法改变数据信息的目的。这种情况经常发生在当 IC 卡与读卡器之间进行数据交换采用加密处理的时候。

在上述描述的攻击方法中，第一种方式是手段，由于 IC 卡是由用户掌握和使用的，管理方无法实现实时跟踪，因此在现实中是无法阻止攻击者进行这种尝试的。第二、三种方式是数据分析处理，是攻击的目的所在。为此，在设计 IC 卡及其相关管理系统时，必须对数据的安全性给予高度重视，从某种角度来说，一个 IC 卡系统设计是否成功，关键在于其对数据安全性的处理。在 IC 卡及系统中使用的都是集成电路卡（IC 卡），集成电路卡的核心是采用集成电路芯片进行数据的存储。目前广泛使用的 IC 卡使用的是电可擦除数据存储芯片（EEPROM），这种芯片读写速度快，掉电后数据可以长期保存，并且数据可以反复进行擦写。IC 卡根据对 EEPROM 读写处理方式的不同，可以分为存储卡、逻辑加密卡以及智能卡（CPU 卡）三大类，它们具有不同的数据保护安全级别。

其中，存储卡是直接将 EEPROM 芯片封装在卡片上，外部设备可以直接访问到 EEPROM 中的任何一个单元。由于存储卡中只有 EEPROM 一个芯片，因此 IC 卡的对外接口实际上就是 EEPROM 的对外接口，这样，外部读写设备就可以十分方便地对 EEPROM 进行数据读写操作，作为 IC 卡而言，无法对合法或非法的读写设备进行判断和识别，非常容易进行攻击。存储卡只是用来对数据进行存储，而无法对数据进行安全性保护，因此存储卡不具备数据安全性保护措施，数据安全级别很低。

而逻辑加密卡是在将 EEPROM 芯片封装在卡片上的同时，将一组硬件逻辑电路也封装在卡片上，外部读写设备必须通过硬件逻辑电路的判断后，才能访问到 EEPROM 中的任何一个单元。由于在 IC 卡中存在一组硬件逻辑加密电路，EEPROM 芯片的接口并不直接对外，在初始状态，IC 卡芯片中的数据开关处于断开状态。外部读写设备在访问 IC 卡芯片中的 EEPROM 单元之前，必须首先发一组数据给硬件逻辑电路，硬件逻辑电路在判断数据的合法性后（即密码校验），才决定是否将 IC 卡内的开关闭合。只有密码校验正确后，硬件逻辑电路才能将开关闭合，这时外部读写设备才能对 EEPROM 中的数据进行读写操作，这样逻辑加密卡就可以对外部合法和非法的读写设备进行识别判断。通过这种方式，逻辑加密卡对内部 EEPROM 中的数据进行了安全性保护，因此逻辑加密卡具备数据安全性保护措施。但逻辑加密卡的安全性级别并不是很高，有两种攻击方式可以对其进行攻击测试：一种是当合法读写设备在发送数据进行密码校验时，非法设备可以跟踪到校验密码，这样，今后非法设备通过重放也可以通过密码校验，从而对逻辑加密卡进行数据攻击；另一种方法是非法设备在跟踪到合法设备已经通过逻辑加密卡的密码校验，IC 卡内部开关闭合后，再通过数据线对逻辑加密卡中 EEPROM 的数据进行攻击破坏。因此，逻辑加密卡虽然具备一定的数据安全性保护，但它的安全级别依然较低。

所以，要保证 IC 卡的安全性，须采用智能卡（CPU 卡）。智能卡是在将 EEPROM 芯片封装在卡片上的同时，将微处理器（CPU）芯片也封装在卡片上，外部读写设备只能通过 CPU 与 IC 卡内的 EEPROM 进行数据交换，在任何情况下都不能再访问到 EEPROM 中的任何一个单元。由于在智能卡中封装了微处理器芯片，这样，EEPROM 的数据接口在

任何情况下都不会与 IC 卡的对外数据线连接。外部读写设备在与智能卡进行数据交换时，首先必须发指令给 CPU，由 CPU 根据其内部 ROM 中存储的卡片操作系统（COS）对指令进行解释，并进行分析判断，在确认读写设备的合法性后，允许外部读写设备与智能卡建立连接。之后的数据操作仍然要由外部读写设备发出相应的指令，并且 CPU 对指令进行正确解释后，允许外部读写设备和智能卡中的数据存储区（RAM）进行数据交换，数据交换成功后，在 CPU 的控制下利用智能卡中的内部数据总线，再将内部 RAM 中的数据与 EEPROM 中的数据进行交换。可以看到，在数据处理过程中，外部读写设备只是和 CPU 打交道，同时数据交换也只能和数据缓存区 RAM 进行，根本无法实现对智能卡中 EEPROM 数据的直接访问，这样就实现了对智能卡 EEPROM 中数据的安全保护。由于智能卡内部具有 CPU 芯片，在具有数据判断能力的同时，也具备了数据分析处理能力，因此智能卡可以随时区别合法和非法读写设备，并且由于有了 CPU 芯片，具备数据运算能力，还可以对数据进行加密解密处理，因此具备非常高的安全性，其安全级别很高。

因此，为了保护 IC 卡的安全，应尽量选用智能卡作为 IC 卡系统的信息传递的介质。

11. 请画出带有时间戳的基于秘密密钥的身份验证过程。

答：Kerberos 身份验证过程如图 3-1 所示。

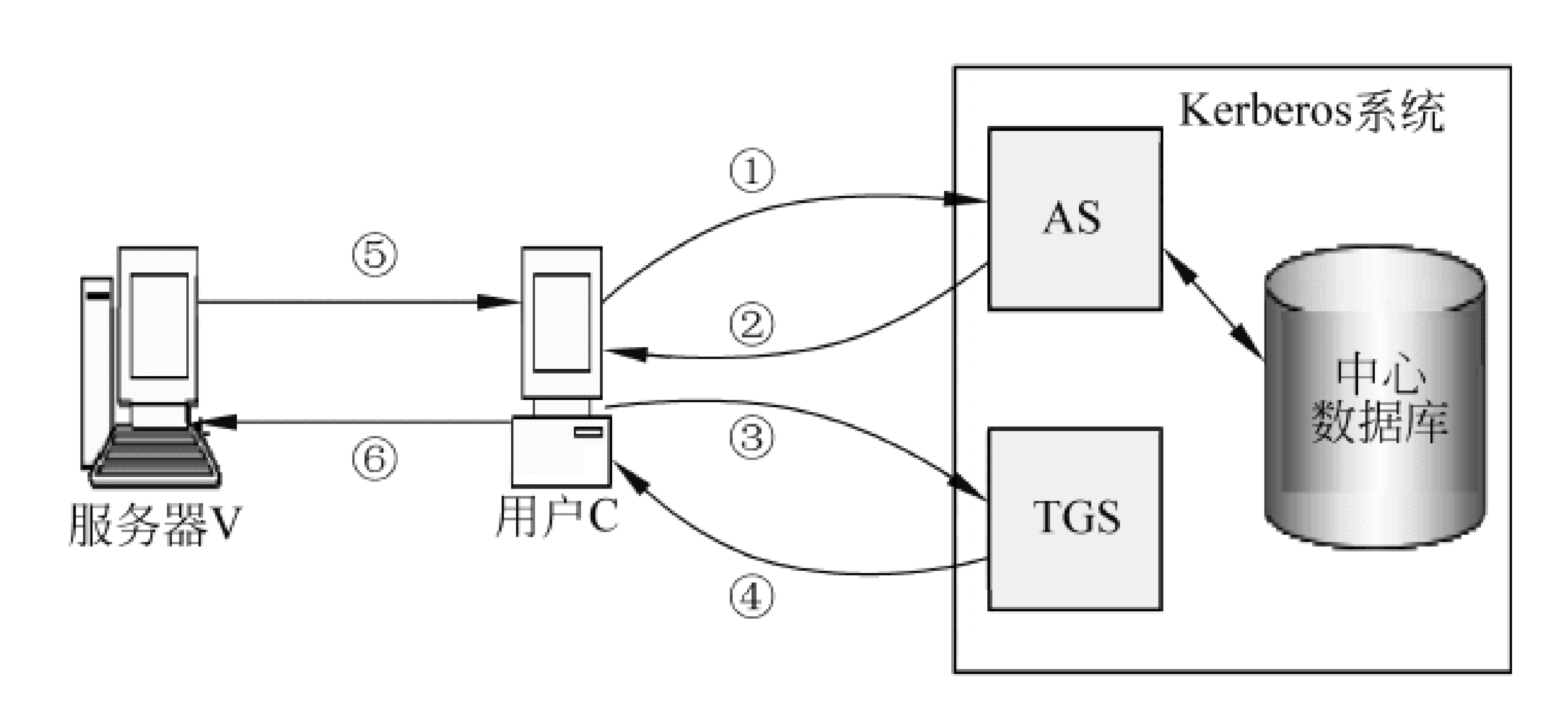


图 3-1　Kerberos 身份验证过程

（1）认证服务交换，用户从 AS 取得入场券。

① 客户向 AS 发出访问 TGS 请求（用 TS_1 表示新请求）：

$$C\rightarrow AS: E_{KC}[ID_C||ID_{TGS}||TS_1]$$

② AS 向 C 发出应答：

$$AS\rightarrow C: E_{KC}[K_C,TGS||ID_{TGS}||TS_2||Lifetime_2||Ticket_{TGS}]$$

其中

$$Ticket_{TGS}=E_{KT}[K_{CT}||ID_C||AD_C\ ||ID_T||TS_2||Lifetime_2]$$

（2）入场券许可服务交换，用户从 TGS 获取服务许可凭证。

③ C 向 TGS 发出请求，内容包括服务器识别码、入场券和一个认证符。

$$C\rightarrow TGS: E_{KCT}[ID_S||Ticket_{TGS}||Authenticator_C\ ]$$

其中

$$Ticket_{TGS}=E_{KT}[K_{CT}|ID_C||AD_C\ ||ID_T||TS_2||Lifetime_2]$$

$$Authenticator_C=E_{KCT}[ID_C||AD_C||TS_3]$$

④ TGS 验证后，向 C 发出服务许可凭证：

$TGS \to C$：$E_{KCT}[K_{CS}||ID_S||TS_4|| Ticket_S]$

其中

$Ticket_S= E_{KTS}[K_{CS}||ID_C||AD_C ||ID_S||TS_4||Lifetime_4]$

（3）客户-服务器相互认证交换，用户从服务器获取服务。

⑤ C 向服务器证明自己身份（用 $Ticket_S$ 和 $Authenticator_C$）

$C \to S$：$E_{KCS}[Ticket_S||Authenticator_C]$

其中

$Ticket_S= E_{KTS}[K_{CS}||ID_C||AD_C ||ID_S||TS_4||Lifetime_4]$

$Authenticator_C= E_{KCS}[ID_C||AD_C||TS_5]$

⑥ 服务器向客户证明自己身份。

$S \to C$：$E_{KCS}[TS_5+1]$

这个过程结束，客户 C 与服务器 S 之间就建立起了共享会话密钥，以便以后进行加密通信或交换新密钥。

12. 简述认证机构的严格层次结构模型的性质。

答：层次结构中的所有实体都信任唯一的根 CA。在认证机构的严格层次结构中，每个实体(包括中介 CA 和终端实体)都必须拥有根 CA 的公钥，该公钥的安装是在这个模型中为随后进行的所有通信进行证书处理的基础，因此，它必须通过一种安全（带外）的方式完成。

值得注意的是，在一个多层的严格层次结构中，终端实体直接被其上层的 CA 认证（也就是颁发证书），但是它们的信任锚是另一个不同的 CA（根 CA）。

13. 证书管理由哪 3 个阶段组成，每个阶段包括哪些具体内容？

答：证书管理的 3 个阶段及具体内容说明如下。

（1）初始化阶段。

A. 终端实体注册

终端实体注册是单个用户或进程的身份被建立和验证的过程。注册过程能够通过不同的方法实现。终端实体注册是在线执行的，是用注册表格的交换说明的。注册过程一般要求包括将一个或更多的共享秘密赋给终端实体，以便后来在初始化过程中 CA 确认那个个体。

B. 密钥对产生

密钥资料可以在终端实体注册过程前或直接响应终端实体注册过程时产生。在 RA 中或在 CA 中产生密钥资料是可能的。每个终端实体多个密钥可以被用作支持分离的和截然不同的服务。例如，一个密钥对可以被用作支持不可否认性服务，而另一个密钥对可以被用作支持机密性或密钥管理功能（双密钥对模型）。

C. 证书创建和密钥/证书分发

无论密钥在哪里产生，证书创建的职责都将单独地落在被授权的 CA 上。如果公钥是被终端实体，而不是 CA 所产生的，那么该公钥必须被安全地传送到 CA，以便其能够被放入证书。

一旦密钥资料和相关的证书已经被产生，它们就必须被适当分发。请求证书和从可信实体（即 CA）取回证书（以及相关的密钥，如果适用的话）的必要条件是要求有一个安全协议机制。

D. 证书分发

如果私钥和相应的公钥证书已经被分发，那么就有一种或多种传送给另一个实体的方法。

- 带外分发。
- 在一个公众的资料库或数据库中公布，以使查询和在线检索简便。
- 带内协议分发。例如，包括带有安全 E-mail 报文的适用的验证证书。

被用作数字签名目的的证书可以仅需要分发给它们的所有者，被用作机密性目的的证书对于发信方必须是容易获得的。

E. 密钥备份和托管

一定比例的加密密钥将因为许多原因（忘记密码、磁盘被破坏、失常的智能卡或雇员被解雇）使这些密钥的所有者无法访问，这就需要事先进行密钥备份。

密钥托管是指把一个秘密的密钥或私钥交由第三方保管，这样做的问题是哪些密钥应委托保管以及谁是可以信任的第三方（政府？）。

（2）颁布阶段。

A. 证书检索

证书检索与访问一个终端实体证书的能力有关。检索一个终端实体证书的需求可能被两个不同的使用要求所驱动。

- 加密发给其他实体的数据的需求。
- 验证一个从另一个实体收到的数字签名的需求。

B. 证书验证

证书验证与评估一个给定证书的合法性和证书颁发者的可信赖性有关。证书验证是在基于那个证书被准许加密操作前进行的。

C. 密钥恢复

密钥管理生命周期包括从远程备份设施（如可信密钥恢复中心或 CA）中恢复私有加密密钥的能力。密钥的恢复能使 PKI 管理员和终端用户的负担减至最小，这个过程必须尽可能最大程度自动化。

D. 密钥更新

当证书被颁发时，其被赋予一个固定的生存期。当证书“接近”过期时，必须颁发一个新的公/私钥和相关证书，这被称为密钥更新。应该允许一个合理的转变时间使依托方取得新证书，从而避免与过期证书所有有关的服务中断。这个过程是自动的，并对终端用户完全透明。

（3）取消阶段。

A. 证书过期

证书在颁布时被赋予一个固定的生存期，在其被建立的有效期结束后，证书将会过期。当一个证书过期后，与该证书有关的终端实体可能发生 3 件事。

- 没有活动：终端实体不再参加 PKI。
- 证书恢复：相同的公钥被加入新有效期的新证书（当与最初证书的颁布有关的环境没有变化时使用，并且它仍然认为是可靠的）。
- 证书更新：一个新的公/私钥对被产生，并且一个新的证书被颁发。

B. 证书撤销

在证书自然过期前对给定证书的即时取消（可疑的密钥损害、作业状态的变化或者雇用终止等）。

一个终端用户个人可以亲自初始化自己的证书撤销（例如，由于相应私有密钥的可疑损害）。RA 可以代表终端用户被用作初始化证书撤销。经授权的管理者也可以有能力撤销终端实体的证书。

C. 密钥历史

由于机密性加密密钥最后要过期，因此可靠安全地存储用作解密的私有密钥是必需的，这被称作密钥历史，否则无法恢复。

D. 密钥档案

可靠地保存已经过期的用于验证数字签名的公钥，以便对历史文档的数字签名进行验证。

14. 简述使用密钥的身份认证的分类方法。

答：有基于公钥加密认证协议的双向认证和单向认证，以及基于单钥加密认证协议的双向认证和单向认证方法。

15. 简述 Kerberos 身份认证的异域认证过程。

答：如图 3-2 所示。

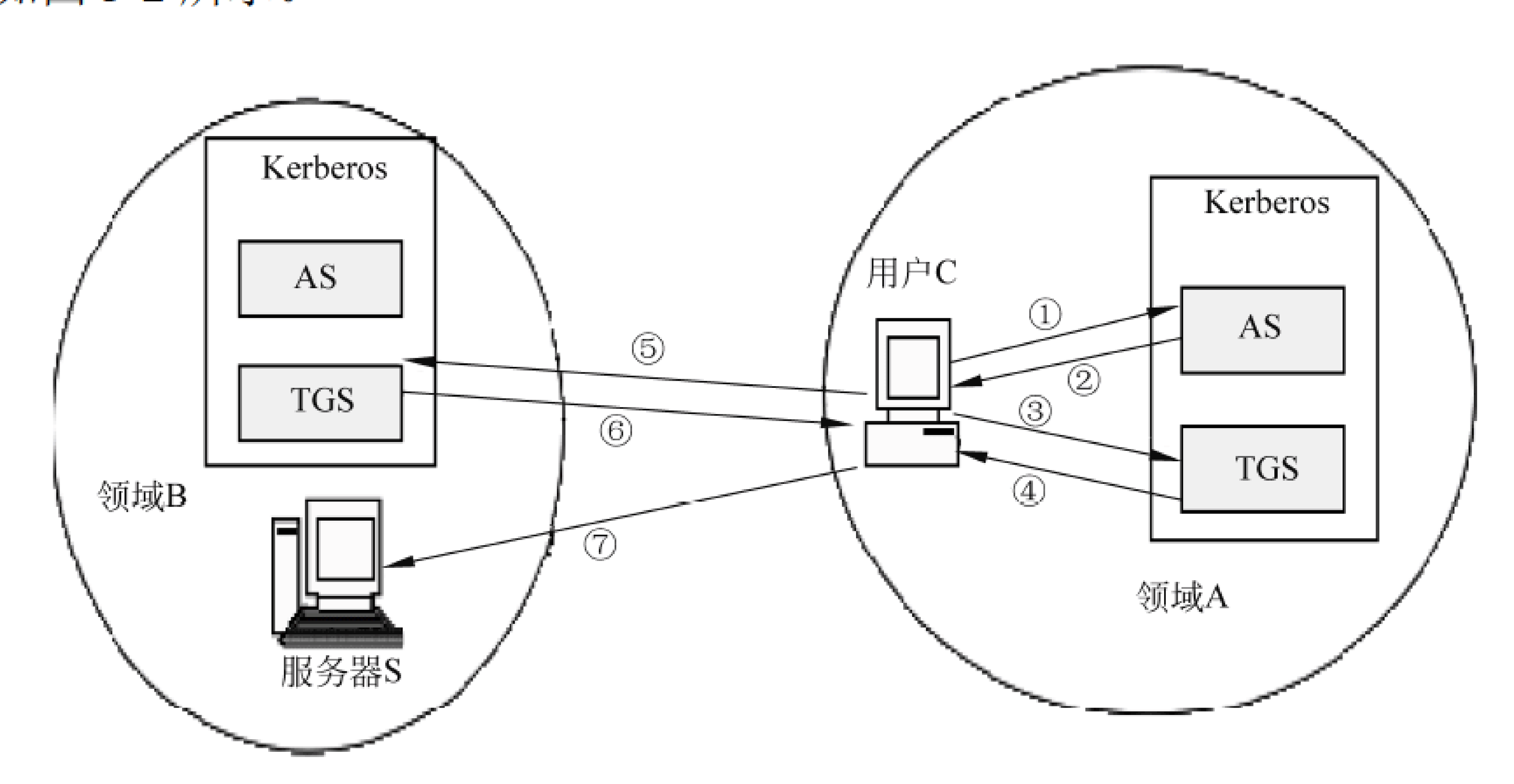


图 3-2 Kerberos 身份认证的异域认证过程

① C→AS：E_{KC} [ID_C || ID_T ||TS_1]。

② AS→C：E_{KC}[K_{CT} ||ID_T || TS_2 || $Lifetime_2$ || $Ticket_{TGS}$]。

③ C→TGS：E_{KCT} [ID_{TB} || $Ticket_{TGS}$ || $Authenticator_C$]（ID_{TB} 为 B 域 TGS_B 标识）。

④ TGS→C：E_{KCT} [K_{CTB}||ID_{TB}||TS_4|| $Ticket_{TB}$] （K_{CTB} 为 C 与 TGS_B 会话密钥）。

$Ticket_{TB}$= E_{KTB}[K_{CTB}||ID_C||AD_C ||ID_{TB}||TS_4||$Lifetime_4$]

⑤ C→TGS_B：E_{KCTB} [ID_{TB}||$Ticket_{TB}$||$Authenticator_C$]。

⑥ TGS_B→C：E_{KCTB} [K_{CS} || ID_{TB} || ||TS_6 || $Ticket_{TB}$]。

⑦ C→S：E_{KCS} [$Ticket_{TB}$||$Authenticator_C$]。

其中，K_C 为 C 的用户主密钥，由 C 上的用户口令导出；可与 AS 共享，记为 K_{CA}。

K_S 为 S 服务器主密钥，可与 TGS 共享，也记为 K_{ST}。

K_T 为 TGS 主密钥，可与 AS 共享，记为 K_{AT}。

K_{CT} 为 C 与 TGS 会话密钥。

K_{TS} 为 TGS 与 S 会话密钥。

K_{CS} 为 C 与 S 会话密钥。

16. 简述 X.509 证书包含的内容。

答：X.509 公开密钥证书包含下列内容。

（1）版本，指明这个证书符合 ITU-T X.509 建议的哪个版本格式。X.509 现在已经有 1，2，3 共 3 个版本。

（2）序列号，由发布证书的 CA 分配。这个序列号在该 CA 发布的所有证书中是唯一的。

（3）算法标识符，指明证书数字签名的算法。

（4）发布者，表明发布和签署该证书的 CA。

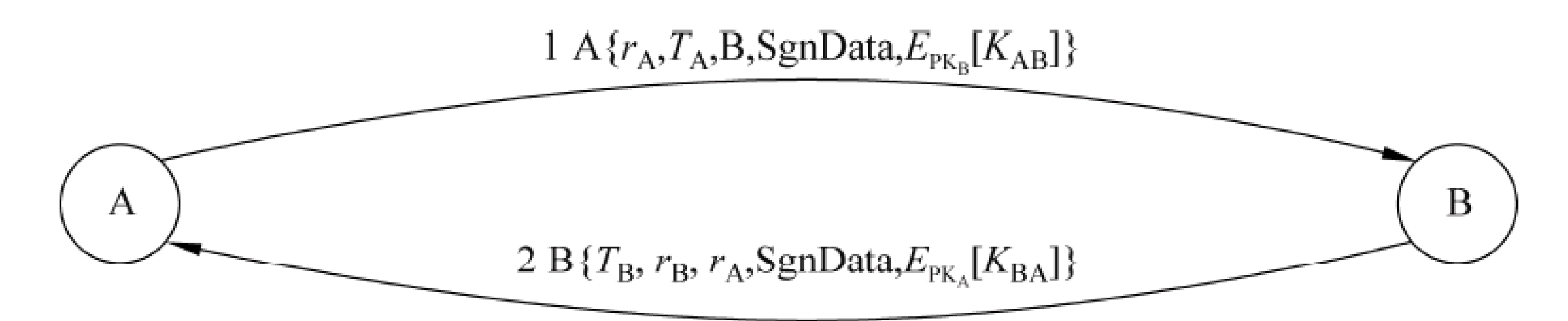
（5）有效期，包含起始两个日期。

（6）主体，定义名字或者是其他的身份标识，表明这个证书发给哪个用户。例如，主体域可能包含名字和住址。

（7）公开密钥信息，包含用户的公开密钥和使用这个密钥的算法。

（8）签名，证书的数字签名。

17. 简述 X.509 的双向认证过程。



答：X.509 建议 3 种认证过程：一次认证（也称单向认证）、二次认证（也称双向验证）和三次认证过程。

双向认证过程即 A 不仅要向 B 发送验证凭证消息，B 也要通过应答证明以下几点：ID_B 的身份，应答是由 B 发出的，应答的接收者是 A，应答报文是完整和及时的。

18. 试述数字证书的原理。

答：数字证书采用公开密钥体制（如 RSA）。每个用户设定一仅为本人所知的私有密

钥，用它进行解密和签名；同时设定一公开密钥，为一组用户所共享，用于加密和验证签名。

采用数字证书，能够确认以下两点。

（1）保证信息是由签名者自己签名发送的，签名者不能否认或难以否认。

（2）保证信息自签发后到收到为止未曾做过任何修改，签发的信息是真实信息。

19. 查阅资料，简述有关 PKI 的标准及其相关产品。

答：PKI 标准：

（1）X.209（1988）ASN.1 基本编码规则的规范。

（2）X.500（1993）信息技术之开放系统互联。

（3）X.509（1993）信息技术之开放系统互联。

（4）PKCS 系列标准。

随着网络应用的不断普及深入，PKI 的市场正在不断扩大。现在，市场上涌现出了很多 PKI 产品，如

（1）Baltimore 公司的 UniCERT。

（2）Entrust 公司的 PKI 产品-Entrust/PKI 5.0。

（3）VeriSign 公司的 OnSite。

20. PKI 可以提供哪些安全服务？PKI 体系中包含了哪些与信任有关的概念？

答：通过数字证书，可以提供身份的认证与识别，完整性、保密性和不可否认等安全服务。在 PKI 中，我们可以把信任定义具体化为：如果一个用户假定 CA 可以把任一公钥绑定到某个实体上，则他信任该 CA。

21. 叙述基于 X.509 的数字证书在 PKI 中的作用。

答：PKI（Public Key Infrastructure）是一个以公开密钥加密法为中心的密钥管理体系结构，它能提供公开密钥加密和数字证书服务，采用证书管理公钥，通过第三方的可信任机构 CA (Certificate Authority)把用户的公钥和用户的其他标识信息（如名称、E-mail、身份证号等）捆绑在一起，在 Internet 上验证用户的身份，即使用数字证书提供用户的公开密钥，让可信任第三方——数字证书认证中心（CA）签署用户的公开密钥。目前广泛认可的 PKI 是以 ITU-T 的 X.509 数字证书第 3 版为基础的结构。

22. 解释访问控制的基本概念。

答：访问控制是建立在身份认证基础上的，通过限制对关键资源的访问，防止非法用户的侵入或因为合法用户的不慎操作而造成的破坏。

访问控制的目的是限制主体对访问客体的访问权限（安全访问策略），从而使计算机系统在合法范围内使用。

23. 访问控制有几种常用的实现方法？它们各有什么特点？

答：（1）访问控制矩阵。

行表示客体（各种资源），列表示主体（通常为用户），行和列的交叉点表示某个主体对某个客体的访问权限。通常，一个文件的 Own 权限表示可以授予（authorize）或撤销（revoke）其他用户对该文件的访问控制权限。

（2）访问能力表。

实际的系统中虽然可能有很多的主体与客体，但两者之间的权限关系并不多。为了减少系统的开销与浪费，可以从主体（行）出发，表达矩阵某一行的信息，这就是访问能力表（capabilities）。

只有当一个主体对某个客体拥有访问能力时，它才能访问这个客体。但是，要从访问能力表获得对某一特定客体有特定权限的所有主体就比较困难。在一个安全系统中，正是客体本身需要得到可靠的保护，访问控制服务也应该能够控制可访问某一客体的主体集合，于是出现了以客体为出发点的实现方式——ACL。

（3）访问控制表。

也可以从客体（列）出发，表达矩阵某一列的信息，这就是访问控制表（Access Control List）。它可以对某一特定资源指定任意一个用户的访问权限，还可以将有相同权限的用户分组，并授予组的访问权。

（4）授权关系表。

授权关系表（authorization relations）的每一行都表示了主体和客体的一个授权关系。对表按客体进行排序，可以得到访问控制表的优势；对表按主体进行排序，可以得到访问能力表的优势。授权关系表适合采用关系数据库实现。

24. 在信息系统内主体通常指什么？客体通常指什么？

答：主体通常指用户，客体通常指资源。

25. 查找资料，分别给出几个自主访问控制、强制访问控制和基于角色的访问控制的实例。

答：（1）“拥有者/同组用户/其他”模式：在 UNIX、Linux、VMS 等系统中，实现了一种十分简单、常用而有效的自主访问控制模式，就是在每个文件上附加一段有关访问控制信息的二进制位，这些二进制位反映了不同类别用户的存取方式，即文件的拥有者、文件拥有者同组的用户和其他用户。

这种模式的一个很大缺点就是，客体的拥有者不能够精确控制某个用户对其客体的访问权，如不能够指定与 owner 同组的用户 A 能够对该客体具有读、写、执行权限，而与 owner 同组的用户 B 不可以对该客体有任何权限。

（2）强制访问控制已经在许多基于安全内核的系统中得以实现，并转换到许多非内核化的操作系统中，包括 Honeywell 公司的 Multics、DEC 公司的 SES/VMS 以及 Sperry 公司的 1100 操作系统。这里，以 UNIX SVR 4.1ES 安全操作系统的强制访问控制机制为例加以说明。

安全操作系统 UNIX SVR 4.1ES 的强制访问控制机制分别对系统中的主体和客体赋予了相应的安全级，并采用了多级安全规则。

A. 主体的安全级。主体的安全级即用户的安全级以及代表用户进行工作的进程的安全级。用户的安全级是系统管理员根据安全策略，使用 adduser 命令创建用户时设置的。系统在用户安全文件档中为每个用户建立一项，表明该用户的安全级范围，并说明其默认安全级。默认安全级在该用户的安全级范围之内。

用户登录系统时，他可以指定本次登录的安全级，指定安全级必须在其安全级范围之内。成功登录后，系统将用户本次指定的安全级设置给为该用户创建的 shell 进程。如果用户不指定登录安全级，系统则将该用户的默认安全级设置给为该用户创建的 shell 进程。

B. 客体的安全级。客体安全级的确定和赋值是根据客体的类型按以下规则进行的文件、有名管道的安全级。文件、有名管道的安全级为创建该客体进程的安全级，且客体的安全级必须等于其父目录的安全级，保存在相应的磁盘 Inode 节点和内存 Inode 节点中。

进程、消息队列、信号量集合和共享存储区的安全级。这组类型的客体不具有文件系统表示形式，其安全级为创建进程的安全级，保存在内存相应的数据索引结构中。

目录的安全级。目录同普通文件一样，在它们的生存周期内具有一个安全级，所不同的是目录的结构须满足兼容性。一个进程创建一个目录，目录的安全级即为创建其进程的安全级，且目录的安全级须大于或等于其父目录的安全级。同文件一样，它保存在相应的磁盘 Inode 节点和内存 Inode 节点中。

C. 设备的安全级。系统在设备安全文档中说明系统中每个设备的安全属性，如设备的最高安全级、最低安全级等。设备还具有当前安全级，一个设备的当前安全级为调用该设备的用户进程、系统进程或系统服务进程的安全级。设备的当前安全级必须在设备的最大安全级与最小安全级之间。

另外，设备分为单级设备和多级设备。多级设备可以包含多个安全级数据。这个设备只能由具有适当特权的进程打开（open），包括内核和系统进程、具有适当特权的管理员进程。磁盘和存储器设备就是多级设备。单级设备在某个时刻只能处理单一安全级的数据。这类设备包括终端和用于某个相应状态的磁带机和软盘驱动器。如果一个设备用作一个公用（public）资源，那么它必须是单级设备。具有适当特权的管理员可以将这些设备用作多级设备，如产生一个系统的磁带备份。

通常，一个用户在登录时访问一个终端设备，这个用户将以某个安全级在该终端上进入系统。如果这个安全级不在这个终端所定义的安全级范围之内，这个登录就会失败。如果登录成功，这个设备的安全级就被设置成用户登录时使用的安全级。

要使用磁带或软盘设备，或者不是在登录时访问终端设备，用户必须要求管理员分配（allocate）设备，管理员以某个安全级将此设备分配给这个用户。如果这个安全级不在设备的安全级范围之内，这个分配将失败。如果成功，用户就成为这个设备的所有者（owner）。此时文件的 DAC 设置为 600，设备安全级为分配命令中给定的安全级，并且管理员将通知用户这个操作已经成功。如果用户当前的安全级等于分配的安全级，用户就可以任意使用这些设备了。

还有少量设备不属于以上两种分类而需要特别处理，包括/dev/null、/dev/zero、/dev/tty。由于数据并不流过这些设备，所以用户随时都可以访问这些设备。

（3）基于角色的访问控制的实例包括北仑国际集装箱码头有限公司基于该控制系统的

软件，包括 *Polaris*（码头生产管理系统）、《费收发票管理系统》《人事工资管理系统》等。基于 RBAC 模型的权限管理系统的实现技术方案简化了开发人员的开发工作，也使用户在进行权限分配时更加直观灵活，并支持岗位、权限多变的需求。

26. 比较自主访问控制、强制访问控制和基于角色的访问控制。

答：自主访问控制（Discretionary Access Control，DAC）由客体的属主对自己的客体进行管理，由属主自己决定是否将自己的客体访问权或部分访问权授予其他主体，这种控制方式是自主的。也就是说，在自主访问控制下，用户可以按自己的意愿，有选择地与其他用户共享他的文件。强制访问控制的基本思想是不允许单个用户确定访问权限，只有系统管理员才可以确定用户或用户组的访问权限。MAC 主要用于多层次安全级别的系统（如军事系统）中。优点是具有更强的访问控制能力，缺点是工作量大，管理不便以及不灵活。基于角色的访问控制（Role-Base Access Control，RBAC）是以角色而非个体设计的访问控制策略，一个个体可以有多重角色，一个角色可以由多人承担，由于角色比个体具有较大的稳定性，这种访问控制比针对个体的自主访问控制和强制访问控制在可操作性和可管理性方面都要强得多。

27. 查找资料，说明还有哪些新的访问控制策略。

答：利用层次分析法，根据用户流量特征对用户的信任度进行评估，采用基于信任度的访问控制策略，并根据信任度动态调整网络防御路径，实现对内部威胁的实时防护。具体实现如下：访问控制应用（ACA）为 SDN 控制器的上层应用，是整个系统的核心。ACA 通过 SDN 控制器获取数据层面的信息和用户的身份信息，通过流量分析设备获得用户的行为信息，并能够从用户信息数据库中获取用户的权限信息。利用层次分析法（Analytic Hierarchy Process，AHP），结合层次结构模型将用户的总体信任度分解为子信任度，再将子信任度分解为更细的数据单元，即信任度证据，然后再从下层到上层进行系统的组合。这种先分解再组合的方法能够解决用户信任评估中的不确定性、主观性。AHP 可分为 5 个步骤：①建立层次结构模型；②构造判断矩阵；③层次单排序及一致性检验；④层次总排序；⑤层次总排序一致性检验。

根据常见的内部威胁类型，将用户总体信任度分解为 5 个子信任度，即身份安全子信任度、越权访问安全子信任度、流量安全子信任度、畸形数据包安全子信任度、扫描攻击安全子信任度。身份安全子信任度主要代表用户身份的可信程度；越权访问安全子信任度主要代表越权访问的严重程度；流量安全子信任度主要代表用户发动流量型攻击的可能性；畸形数据包安全子信任度代表用户发动畸形包攻击的可能性；扫描攻击安全子信任度代表用户扫描网络中主机和端口的可能性。

通过层次分析法可以得到总体信任度和 5 个子信任度的值。上述 6 个信任度值作为系统选取访问控制策略的依据。系统每隔一段时间计算一次信任度的值，并根据得到的信任度决定是否需要进行访问控制策略的变更。

第 4 章　网络安全防护

4.1　第 4 章知识提要

本章习题详细解答了关于防火墙、Internet 安全协议、VPN、入侵检测系统、网络诱骗、蜜罐技术等方面的常见问题和实践思路。

4.2　第 4 章习题和答案详解

一、选择题（答案：BCADC BDBDD DBACA DABBC CADDA）

1．防火墙用于将Internet和内部网络隔离，是________。

A. 防止Internet火灾的硬件设施
B. 网络安全和信息安全的软件和硬件设施
C. 保护线路不受破坏的软件和硬件设施
D. 起抗电磁干扰作用的硬件设施

答案：B

解答：防火墙的主要作用是保护系统安全，由硬件和软件联合实现。

2. 防火墙最主要被部署在________位置。

A. 网络边界
B. 骨干线路
C. 重要服务器旁
D. 桌面终端

答案：C

解答：根据题意，防火墙主要被部署在重要服务器旁最切合答案。

3. 下列关于防火墙的说法中错误的是________。

A. 防火墙工作在网络层
B. 防火墙对IP数据包进行分析和过滤
C. 防火墙是重要的边界保护机制
D. 部署防火墙，就解决了网络安全问题

答案：A

解答：目前的硬件防火墙可以在第二层至第七层工作，即可以作链路层访问控制（MAC）到应用层访问控制（关键字过滤等），不只是在网络层，因此选A。

4. 在一个企业网中，防火墙应该是________的一部分，构建防火墙时首先要考虑其保护的范围。

A. 安全技术

B. 安全设置

C. 局部安全策略

D. 全局安全策略

答案：D

解答：防火墙是全局安全策略的一部分。

5. 一般而言，Internet防火墙建立在一个网络的________。

A. 内部子网之间传送信息的中枢

B. 每个子网的内部

C. 内部网络与外部网络的交叉点

D. 部分内部网络与外部网络的结合处

答案：C

解答：一般而言，Internet防火墙建立在一个网络的内部网络与外部网络的交叉点。

6. 包过滤型防火墙从原理上看是基于________进行数据包分析的技术。

A. 物理层

B. 数据链路层

C. 网络层

D. 应用层

答案：B

解答：根据包过滤型防火墙的定义，应该选B。

7. 对非军事DMZ而言，正确的解释是________。

A. DMZ是一个真正可信的网络部分

B. DMZ网络访问控制策略决定允许或禁止进入DMZ通信

C. 允许外部用户访问DMZ系统上合适的服务

D. 以上3项都是

答案：D

解答：对非军事DMZ而言，正确的解释是 DMZ是一个真正可信的网络部分，DMZ网络访问控制策略决定允许或禁止进入DMZ通信，允许外部用户访问DMZ系统上合适的服务，所以选D。

8. 对动态网络地址交换（NAT），不正确的说法是________。

A. 将很多内部地址映射到单个真实地址

B. 外部网络地址和内部地址一对一地映射
C. 每个连接使用一个端口
D. 最多可有64 000个同时的动态NAT连接

答案：B

解答：对动态网络地址交换（NAT），外部网络地址和内部地址不是一对一的映射，借助于NAT，私有（保留）地址的“内部”网络通过路由器发送数据包时，私有地址被转换成合法的IP地址，一个局域网使用少量IP地址（甚至1个）即可实现私有地址网络内所有计算机与Internet的通信需求，因此选B。

9. 以下________不是包过滤防火墙主要过滤的内容。
A. 源IP地址
B. 目的IP地址
C. TCP源端口和目的端口
D. 时间

答案：D

解答：包过滤防火墙主要过滤的内容不包括时间，因此选D。

10. 在被屏蔽的主机体系中，堡垒主机位于________中，所有的外部连接都经过滤路由器到它上面去。
A. 内部网络
B. 周边网络
C. 外部网络
D. 自由连接

答案：D

解答：在被屏蔽的主机体系中，堡垒主机位于自由连接处。

11. 外部数据包经过过滤路由只能阻止________的唯一IP欺骗。
A. 内部主机伪装成外部主机IP
B. 内部主机伪装成内部主机IP
C. 外部主机伪装成外部主机IP
D. 外部主机伪装成内部主机IP

答案：D

解答：外部数据包经过过滤路由只能阻止外部主机伪装成内部主机IP的唯一IP欺骗。

12. IPSec协议工作在网络的________。
A. 数据链路层
B. 网络层
C. 应用层

D. 传输层

答案：B

解答：IPSec协议工作在网络的网络层。

13. IPSec协议中涉及密钥管理的重要协议是________。

A. IKE

B. AH

C. ESP

D. SSL

答案：A

解答：IPSec协议中涉及密钥管理的重要协议IKE（Internet Key Exchange）。

14. SSL产生会话密钥的方式是________。

A. 从密钥管理数据库中请求获得

B. 每一台客户机分配一个密钥的方式

C. 随机由客户机产生并加密后通知服务器

D. 由服务器产生并分配给客户机

答案：C

解答：SSL产生会话密钥的方式是：随机由客户机产生并加密后通知服务器。

15. 传输层保护的网络采用的主要技术是建立在________基础上的________。

A. 可靠的传输服务　安全套接字层（SSL）协议

B. 不可靠的传输服务　S-HTTP

C. 可靠的传输服务　S-HTTP

D. 不可靠的传输服务　安全套接字层（SSL）协议

答案：A A

解答：传输层保护的网络采用的主要技术是建立在可靠的传输服务基础上的安全套接层（SSL）协议。

16. 主要用于加密机制的协议是________。

A. HTTP

B. FTP

C. Telnet

D. SSL

答案：D

解答：主要用于加密机制的协议是SSL。

17. 通常所说的移动VPN是指________。

A. Access VPN
B. Intranet VPN
C. Extranet VPN
D. 以上均不是

答案：A

解答：通常所说的移动VPN是指 Access VPN。

18. 以下属于第二层的VPN隧道协议有________。
A. IPSec
B. PPTP
C. GRE
D. 以上均不是

答案：B

解答：属于第二层的VPN隧道协议有PPTP。

19. 将公司与外部供应商、客户及其他利益相关群体相连接的是________。
A. 内联网VPN
B. 外联网VPN
C. 远程接入VPN
D. 无线VPN

答案：B

解答：将公司与外部供应商、客户及其他利益相关群体相连接的是外联网VPN。

20. 以下不属于隧道协议的是________。
A. PPTP
B. L2TP
C. TCP/IP
D. IPSec

答案：C

解答：TCP/IP 不属于隧道协议。

21. 以下不属于VPN核心技术的是________。
A. 隧道技术
B. 身份认证
C. 日志记录
D. 访问控制

答案：C

解答：日志记录不属于VPN核心技术。

22. ________通过一个拥有与专用网络相同策略的共享基础设施，提供对企业内部网或外部网的远程访问。

A. Access VPN

B. Intranet VPN

C. Extranet VPN

D. Internet VPN

答案：A

解答： Access VPN通过一个拥有与专用网络相同策略的共享基础设施，提供对企业内部网或外部网的远程访问。

23. L2TP隧道在两端的VPN服务器之间采用________验证对方的身份。

A. SSL

B. 数字证书

C. Kerberos

D. 口令握手协议CHAP

答案：D

解答： L2TP隧道在两端的VPN服务器之间可以采用口令握手协议CHAP验证对方的身份。

24. 入侵检测的基本方法是________。

A. 基于用户行为概率统计模型的方法

B. 基于神经网络的方法

C. 基于专家系统的方法

D. 以上都正确

答案：D

解答： 入侵检测的基本方法是包括基于用户行为概率统计模型的方法、基于神经网络的方法、基于专家系统的方法等多种方法，所以选D。

25. 关于入侵检测技术，下列描述中错误的是________。

A. 入侵检测系统不对系统或网络造成任何影响

B. 审计数据或系统日志信息是入侵检测系统的一项主要信息来源

C. 入侵检测信息的统计分析有利于检测到未知的入侵和更为复杂的入侵

D. 基于网络的入侵检测系统无法检查加密的数据流

答案：A

解答： 入侵检测系统会对系统或网络造成影响，因此选A。

二、填空题

答案：1. 内外网，内部网，外部网

2. 双宿主机，屏蔽主机，屏蔽子网
3. 主机，网络，分布式
4. 隧道

1. 防火墙位于 内外网 之间，一端是 内部网 ，另一端是 外部网 。
2. 防火墙系统的主要体系结构有 双宿主机 体系结构、 屏蔽主机 体系结构和 屏蔽子网 体系结构。
3. 按检测的监控位置划分，入侵检测系统可分为基于 主机 的入侵检测系统、基于 网络 的入侵检测系统和 分布式 入侵检测系统。
4. 隧道 被定义为通过公用网络建立一个临时的、安全的连接，是一条穿过公用网络的安全、稳定的通道。

三、问答题

1. 在组建 Intranet 时，防火墙是必需的吗？为什么？

答：是的。因为 Intranet 称为企业内部网，或称内部网、内联网、内网，是一个使用与因特网同样技术的计算机网络，它通常建立在一个企业或组织的内部并为其成员提供信息的共享和交流等服务，可以说 Intranet 是 Internet 技术在企业内部的应用。它需要建立防火墙把内部网和 Internet 分开，以保证内部网的高安全性。当然，Intranet 并非一定要和 Internet 连接在一起，它完全可以自成一体作为一个独立的网络。

2．试述一个防火墙产品应具备哪些基本功能。

答：防火墙主要用于保护内部安全网络免受外部不安全网络的侵害，但也可用于企业内部各部门网络之间，限制它们的互相访问。

防火墙对流经它的网络通信进行扫描，这样能够过滤掉一些攻击，以免其在目标计算机上被执行。防火墙还可以关闭不使用的端口，而且它还能禁止特定端口的流出通信，封锁特洛伊木马。最后，它可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。

总之，一个防火墙产品应该具备强化网络安全策略，防止故障蔓延，对网络访问进行监控审计和报警，提供流量控制和计费，实现 MAC 和 IP 地址的绑定等基本功能。

3. 下面是选择防火墙时应考虑的一些因素，请按你的理解，将它们按重要性排序。

（1）被保护网络受威胁的程度。
（2）受到入侵，网络的损失程度。
（3）网络管理员的经验。
（4）被保护网络的已有安全措施。
（5）网络需求的发展。
（6）防火墙自身管理的难易度。
（7）防火墙自身的安全性。

答：7145623

4. 列举更多的防火墙系统结构，最好有自己的创意。

答：已有防火墙主要的体系结构：

1）包过滤型防火墙

优点：

（1）处理数据包的速度较快（与代理服务器相比）。

（2）实现包过滤几乎不再需要费用。

（3）包过滤路由器对用户和应用来说是透明的。

缺点：

（1）包过滤防火墙的维护较困难。

（2）只能阻止一种类型的 IP 欺骗。

（3）任何直接经过路由器的数据包都有被用作数据驱动式攻击的潜在危险，一些包过滤路由器不支持有效的用户认证，仅通过 IP 地址判断是不是安全的。

（4）不能提供有用的日志或者根本不能提供日志。

（5）随着过滤器数目的增加，路由器的吞吐量会下降。

（6）IP 包过滤器可能无法对网络上流动的信息提供全面的控制。

2）双宿/多宿主机防火墙

优点：

（1）可以将被保护的网络内部结构屏蔽起来，增强网络的安全性。

（2）可用于实施较强的数据流监控、过滤、记录和报告等。

缺点：

（1）使访问速度变慢。

（2）提供服务相对滞后或者无法提供。

3）被屏蔽主机防火墙

优点：

（1）其提供的安全等级比包过滤防火墙系统要高，实现了网络层安全（包过滤）和应用层安全（代理服务）。

（2）入侵者在破坏内部网络的安全性前，必须首先渗透两种不同的安全系统。

（3）安全性更高。

缺点：路由器不被正常路由。

4）被屏蔽子网防火墙

优点：安全性高，若入侵者试图破坏防火墙，他必须重新配置连接 3 个网的路由，既不切断连接，同时又不使自己被发现，难度系数高。

缺点：

（1）不能防御内部攻击者，来自内部的攻击者是从网络内部发起攻击的，他们的所有攻击行为都不通过防火墙。

（2）不能防御绕过防火墙的攻击。

（3）不能防御全新的威胁，防火墙只能用来防备已知的威胁。

（4）不能防御数据驱动的攻击。

5）其他防火墙体系结构

最近提出的新型智能防火墙与传统防火墙比较，传统防火墙是利用简单的机制，机械地执行安全策略，过滤规则相对固定、网络信息的捕获能力和处理能力差、依赖人工干预才能响应新的变化。因此，它们不能有效地解决目前新的网络安全问题。而新一代的学习型智能防火墙借助人工智能的思想，弥补了传统防火墙的不足，自身的安全性有了很大提高，在特权最小化、系统最小化、内核安全、系统加固、系统优化和网络性能最大化方面，与传统型防火墙相比有质的飞跃。

5. 查找资料，叙述防火墙测试的内容和方法。

答：首先建立测试准则，搭建测试环境，确定测试项目，进行测试。

举例说明：防火墙设备测试采用 4 个万兆接口，接口为光口，同时支持 850nm 多模和 1310nm 单模光纤接入。L2-L3 层测试流量为 30GB，TCP 并发连接须达到 1000 万。防火墙需配置在 NAT 模式下进行测试。

A. 测试项目：L2-3_吞吐量测试。

测试目的：测试网络安全设备通过 L2 或 L3 的非状态流量的最大流量，即吞吐量，使用 UDP 不基于状态基的报文作为测试流量。

测试拓扑（图 4-1）：

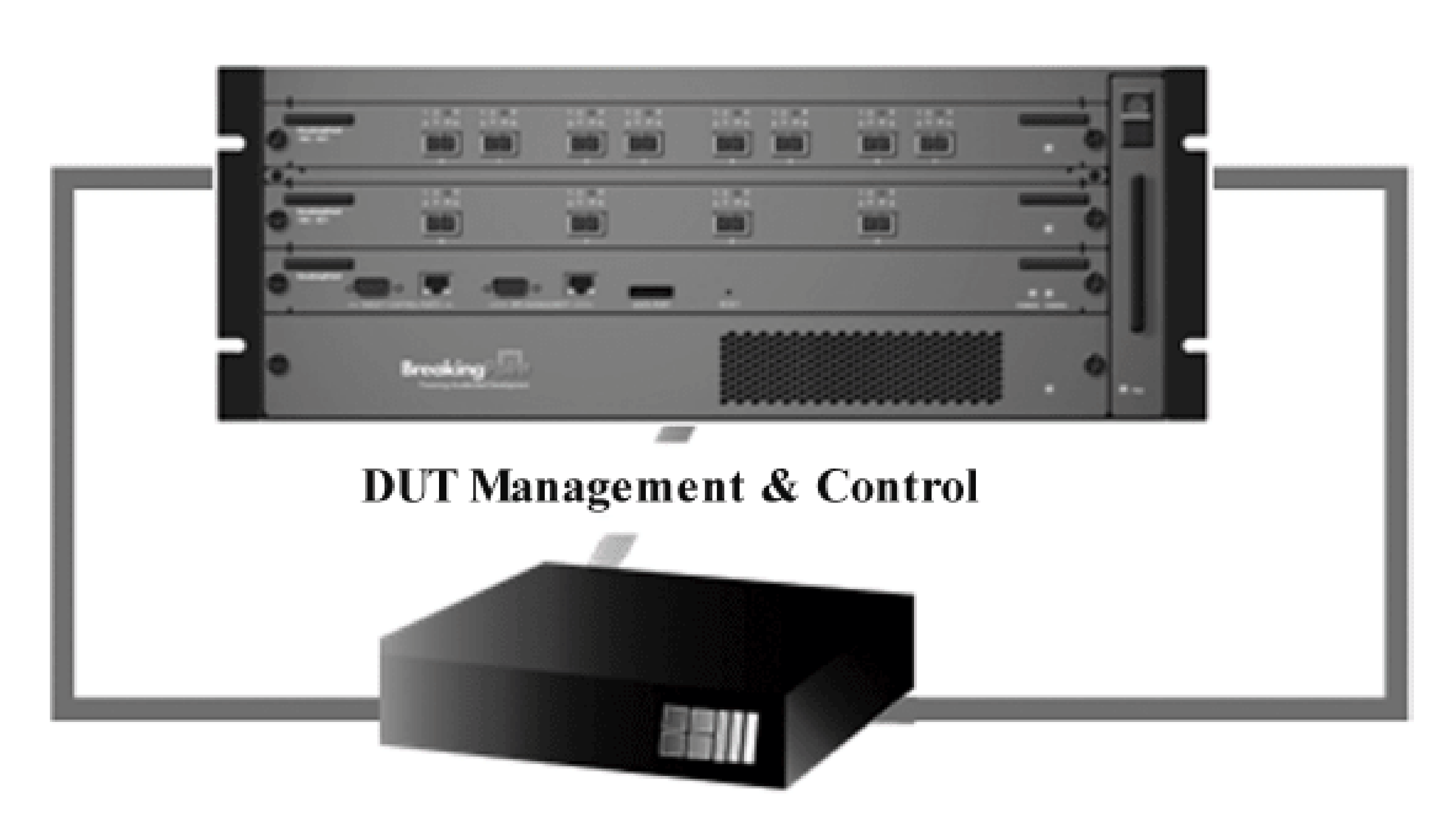


图 4-1　防火墙性能测试简图

测试思路：

（1）将防火墙的 4 个 10G 端口与测试仪的 4 个 10G 端口分别连接。

（2）按照 RFC2544 标准规定，选择 1514B 长度进行测试。

（3）测试仪总共发送 30Gb/s 的双向流量进行测试。

（4）分别使用单模和多模的 XFP 模块进行测试。

（5）观察流量的丢包情况。

测试预期：在 30GB 流量的压力测试下，防火墙能够正确转发，没有丢包。

B. 测试项目：L2-3_时延测试。

测试目的：测试网所产生时延。使用 UDP 不基于状态基的报文作为测试流量

测试拓扑同图 4-1。

测试思路：

（1）将防火墙的 4 个 10G 端口与测试仪的 4 个 10G 端口分别连接。

（2）按照 RFC2544 标准规定，选择 1514B 长度进行测试。

（3）测试仪总共发送 30Gb/s 的双向流量进行测试。

（4）分别使用单模和多模的 XFP 模块进行测试。

（5）观察收发时延。

测试预期：网络周边设备延迟不超过 1ms，核心设备延迟不超过 300μs。

C. 测试项目：L4_TCP 最大并发连接数测试。

测试目的：测试网络安全设备最大的 TCP 并发连接数。

测试拓扑同图 4-1。

测试思路：

（1）无数据传输时最大 TCP 连接数理论值测试是测试在没有应用数据传送情况下的最大 TCP 连接数，通常这种流量在现实网络不会出现，但它可以反映 DUT 能承受的最大连接数。

a. 仪表一个端口模拟客户端，另一个端口模拟服务器端。

b. 由客户端按照一定的每秒连接数向服务器端发起 TCP 连接请求。

c. 客户端与服务器端将不断建立新的连接。

d. 当客户端与服务器之间的 TCP 连接超过防火墙的极限值时，新的连接将不能再建立。

e. 此时的连接数即为最大 TCP 连接数的理论值。

（2）有数据传输时最大 TCP 连接数理论值是测试在有应用数据传送情况下的最大 TCP 连接数。

a. 仪表的一个端口模拟客户端，另一个端口模拟服务器端。

b. 由客户端按照一定的每秒连接数向服务器端发起 TCP 连接请求。

c. 客户端与服务器端将不断建立新的连接。

d. 当客户端与服务器之间的 TCP 连接超过防火墙的极限值时，新的连接将不能再建立。

e. 此时按照一定的数据段大小传送 1GB 的数据流，观察是否可以顺利传送。

（3）基于状态的最大 TCP 连接数。

a. 仪表的一个端口模拟客户端，另一个端口模拟服务器端。

b. 由客户端按照一定的每秒连接数向服务器端发起 TCP 连接请求。

c. 客户端与服务器端将不断建立新的连接。

d. 观察 TCP session 的状态机。

测试预期：防火墙应能承受 1000 万 TCP 并发连接。

其他测试内容还包括测试项目每秒 TCP 最大新建连接数、TCP 平均建立时间分布、二/三层基准转发测试、TCP 平均响应报文时间、TCP 平均关闭时间、应用层典型带宽混合业务吞吐量、应用响应时间测试、SYN_Flood 测试、UDP_Flood 测试、ICMP_Flood 测试、设备的稳定性测试、100 条策略设备的稳定性测试、正常流量转发中增加策略的测试等。

6. 查找资料，叙述防火墙选型的基本原则和具体标准。

答：没有一个防火墙的设计能够适用于所有环境，因此，在选择防火墙时，应根据网络和站点的特点选择。如果站点对保密性要求高，就应该选择有强大认证功能的防火墙，如代理服务或混合型防火墙；如需要较高的网络通信效率，网络接入带宽较高，又只需保障基本的安全性能，则包过滤是较好的选择；如果站点连接到因特网上仅是为了接收电子邮件，则根本不需要防火墙。

在决定用防火墙实施网络的安全策略后，不管具体的实施原理是什么，良好的防火墙一般应具备以下功能：

（1）本身支持安全策略；当网络的安全策略改变时，就可加入新服务。

（2）必要时能运用过滤技术允许和禁止服务；有先进的认证手段，或可以安装先进的认证方法。

（3）能支持“除非明确允许，否则就禁止”的设计策略；可使用 FTP 和 Telnet（远程登录）等服务代理；能根据数据包的性质进行包过滤；允许公众对站点的访问。

（4）能把信息服务器和其他内部服务器分开。

7. 简述攻击防火墙的主要手段。

答：一般来说，防火墙的抗攻击性很强，可是它也不是不可攻破的。防火墙也是由软件和硬件组成的，在设计和实现上都不可避免地存在着缺陷。举例说明：攻击数据包过滤防火墙。

包过滤防火墙是最简单的一种，它在网络层截获网络数据包，根据防火墙的规则表检测攻击行为。它根据数据包的源 IP 地址、目的 IP 地址、TCP/UDP 源端口、TCP/UDP 目的端口过滤，很容易受到如下攻击。

A．IP 欺骗攻击

IP 欺骗攻击主要是修改数据包的源、目的地址和端口，模仿一些合法的数据包骗过防火墙的检测。如外部攻击者将他的数据报源地址改为内部网络地址，防火墙看到是合法地址就放行了。防止 IP 欺骗的方法是在网络的入口和出口点设置包过滤器，外部入口点过滤器明确拒绝所有声称来自内部网络主机的入站包，内部出口点过滤器则只允许来自内部网络主机的出站包，也就是使用防火墙结合接口、地址匹配，达到防止攻击的目的。

B．拒绝服务攻击

简单的包过滤防火墙不能跟踪 TCP 的状态，很容易受到拒绝服务（Denial of Service，DoS）攻击，一旦防火墙受到 DoS 攻击，可使正在使用的计算机出现无响应、死机的现象。这种攻击行为通过发送一定数量一定序列的报文，使网络服务器中充斥了大量要求回复的信息、消耗网络带宽或系统资源，导致网络或系统不胜负荷，以致瘫痪、停止正常的网络服务。常用的攻击软件有同步洪流、WinNuke、死亡之 PING、Echl 攻击、ICMP/ SMURF、Finger 炸弹、Land 攻击、Ping 洪流、Rwhod、tearDrop、TARGA3、UDP 攻击、OOB 等。

对策：通过限制系统可接受的 TCP 连接个数及缩短连接保持在半开状态的时间（即 TCP 的三次握手已经初始化但没有最终完成的那段时间），可以降低或消除 SYN 溢出攻击所带来的影响，还可以限制 Ping 包的大小，使在重组 IP 分段时不发生溢出。

C. 协议隧道攻击

协议隧道的攻击思想类似于 VPN 的实现原理，攻击者将一些恶意的攻击数据包隐藏在一些协议分组的头部，从而穿透防火墙系统对内部网络进行攻击。例如，许多允许 ICMP 回射请求、ICMP 回射应答和 UDP 分组通过的防火墙就容易受到 ICMP 和 UDP 隧道的攻击。Loki 和 lokid(攻击的客户端和服务端) 是实施这种攻击的有效工具。在实际攻击中，攻击者首先必须设法在内部网络的一个系统上安装 lokid 服务端，而后攻击者就可以通过 loki 客户端将希望远程执行的攻击命令(对应 IP 分组)嵌入在 ICMP 或 UDP 包头部，再发送给内部网络服务端 lokid，由它执行其中的命令，并以同样的方式返回结果。由于许多防火墙允许 ICMP 和 UDP 分组自由出入，因此攻击者的恶意数据就能附带在正常的分组，绕过防火墙的认证，顺利地到达攻击目标主机。启动 lokid 服务器程序的命令：lokid-p- I- vl。启动 loki 客户程序的命令：loki-d172.29.11.191（攻击目标主机）- p- I- v1- t3。这样，lokid 和 loki 就联合提供了一个穿透防火墙系统访问目标系统的一个后门。

D. 利用 FTP- pasv 绕过防火墙认证的攻击

目前很多防火墙不能过滤这种攻击手段，如 Checkpoint 的 Firewall-1 在监视 FTP 服务器发送给客户端的包的过程中，它在每个包中寻找“227”这个字符串。如果发现这种包，将从中提取目标地址和端口，并对目标地址加以验证。通过后，将允许建立到该地址的 TCP 连接。攻击者通过这个特性，可以设法连接受防火墙保护的服务器和服务。

E. CGI 漏洞攻击

CGI 即通用网关接口，是外部程序和 HTTP 服务器进行信息交互的一种标准。由于它是实时执行的，所以返回的信息也是动态的，它也是当前网络上应用最广的 Web。由于防火墙必须开放 Web 服务，利用 CGI 问题突破防火墙的防护，部分或全部控制服务器成为攻击防火墙的重要手段。

CGI 的安全问题主要有两个方面：一是 Web 服务器的安全问题，包括 Web 服务器软件设计中的 Bug 及服务器配置错误，这些错误会引起 CGI 源代码泄露、物理路径信息泄露、系统敏感信息泄露或可以远程执行任意指令等安全问题。二是 CGI 语言的安全问题，这类问题较多，如 CGI 程序和数据文件的权限设置不当可能导致 CGI 源代码和敏感信息泄露；CGI 程序的边界条件错误可能被攻击者利用发起缓冲区溢出攻击；访问验证错误导致未授权访问，修改甚至删除没有访问权限的内容；来源验证错误被攻击者利用进行拒绝访问数据给受攻击者。简言之，攻击者观察和控制着受攻击者在 Web 上做的每一件事。目前在各种系统中，CGI 程序的安全漏洞数不胜数，如/ cgi-bin 目录下的 count.cgi 程序（wwwcount 2.3 版）中有一个溢出错误，允许入侵者无须登录便能远程执行任何指令；在/scripts/ tools/目录下的 uploadx.asp 程序，只要入侵者有一个可用账号，哪怕是 guest 账号，也可以上传任何文件到 Web 目录，除替换主页外，还可以进一步控制整个系统。许多黑客软件可以实现 CGI 漏洞或绕过防火墙设置 CGI 后门，如软件 Voideye 2000 可以扫描 119 个 CGI 漏洞，软件 Twwwscan V1.2 可以扫描 400 多个 WWW/CGI 漏洞，而软件 cgi-backdoor 可以绕过防火墙在主机上放置 CGI 木马。

采取以下策略有助于加强 CGI 的安全：正确配置服务器；正确安装 CGI 程序，删除不必要的安装文件和临时文件；编写 CGI 程序时使用安全的函数；使用安全有效的用户身

份验证方法；过滤特殊字符；培养良好的编程习惯等。

8. 查找资料，简述目前国内外防火墙技术发展的现状和自己对防火墙的未来的设想。

答：防火墙技术的发展现状分 4 种，具体说明如下。

（1）包过滤技术：该项技术主要经历了 4 个阶段的发展。首先是静态包过滤防火墙，即传统的边界防火墙的发展，它和路由器同时出现，此技术虽简单、透明、高速，但在安全性能上没有很好的保障。

（2）动态包过滤技术，该技术解决了存在于静态包过滤技术的安全限制问题，也提供了更好的性能，在目前应用较普遍，但随主动攻击的增长，该技术也将面临巨大的挑战。

（3）全状态检测防火墙技术，该技术对传输层的控制能力有了很大的提高，通过采用一系列优化技术改进了流量的处理速度，使其性能得到大幅提升，是当前的主流技术。

（4）深度包检测防火墙技术，该技术通过指纹匹配、异常检测、启发式和统计学分析技术等对数据包进行处理。它能阻止 DDoS 攻击、病毒传播，解决高级应用入侵问题。该项技术一定程度上代表了防火墙技术的发展方向。

防火墙技术未来发展趋势包括以下 3 个方面。

（1）包过滤技术的发展方向，首先应开发使用多级过滤技术，对 URL 及内容进行有效过滤，很好地对 IP 源地址、数据包及进出网络的内容检测，这种综合型过滤技术的应用有利于防火墙技术的扩展。其次是加强防火墙技术的病毒防护能力，有效遏止病毒的网络传播，为网络用户减少损失。

（2）防火墙体系结构的发展方向，我们需要开发一种防火墙，能提高数据处理的效率，使数据通过防火墙时受到的延迟足够小，减轻 CPU 的负担，并能够高效、灵活运用。

（3）防火墙系统管理体系的发展方向，首先是集中式管理，分层的安全结构及分布式发展是将来的趋势，这样既可以使管理成本降低，也能保证大型网络的安全。其次是审计和日志的自动分析功能要增强，以便于及时发现安全漏洞、潜在的威胁和可能的攻击性行为，加强网络的安全管理。

另外，新一代智能防火墙技术需要得到研究与发展，以能更好地保证信息安全，保障网络高效应用。

9. 收集资料，对当前常用的防火墙产品进行分析比较，详细描述其中的 3 种防火墙产品的用法以及升级方法。

答：除了常用的包过滤、应用代理和混合型防火墙外，全状态检测防火墙（full state inspection）是由一个知名防火墙厂家 Checkpoint 提出的一种新型防火墙，据 Checkpoint 关于 Firewall-1 技术文档的介绍，该种防火墙既能具有包过滤的功能，又能具有代理防火墙的安全性。Firewall-1 拥有一个强大的检测模块（inspection model），该模块可以分析所有的包通信层，并提取相关的通信及应用状态信息。Firewall-1 的检查模块位于操作系统的核心，位于链路层和网络层之间，因此，任何包未通过该模块检验之前将不会交给更高的协议层处理。据说状态检测可以支持所有主要的因特网服务和上百种应用程序，如 E-mail、FTP、Telnet、Oracle SQL*Net 数据库存取和新兴的多媒体应用程序，如 RealAudio、VDOLive。

还有，自适应代理防火墙是 Network Associate 公司提出的新一代防火墙。在自适应防火墙中，在每个连接通信的开始仍然需要在应用层接受检测，而后面的包可以经过安全规则由自适应代理程序自动选择是使用包过滤，还是代理。自适应代理模块是依靠动态包过滤模块得知通信连接的情况，当一个连接到来时，动态包过滤将通知代理并提供源和目的的信息，然后自适应代理根据管理员关于“安全与性能”选择的配置灵活地为每个连接指定相应的策略。

在自适应代理中，动态包过滤允许代理要求新连接的通知，接着代理就可以检查每个具体的连接信息，告诉动态包过滤接下去应该对该包做如何处理，如丢弃，转发还是将包提到应用层检查。动态包过滤对每个连接采用的过滤规则都是由代理自动调整的。

虽然 Network Associate 的这套自适应代理技术具有一定的先进性，但据说并未完全被该公司所实现，因此该公司的技术文档中很难有关于自适应代理的详细资料。由于国外的网络安全要比国内发展得早，而且国外的软硬件技术水平也要比国内高，因此国外的防火墙产品自然比国内的产品更加成熟和先进。所以，这里将国外防火墙中运用的先进技术提出来加以分析。这些技术可分成以下三大类。

（一）性能实现

随着网络速度的不断提升，防火墙的性能越来越成为国外厂家关注的问题，他们一般从硬件、操作系统和检测方法方面作改进。

（1）专用硬件。

使用专用的硬件以 NetScreen 防火墙最为典型，NetScreen 防火墙之所以具有很好的性能，是和采用专用硬件设计分不开的。在每个 NetScreen 设备中，都有 ASIC（Application Specific Integrated Circuit）芯片，这些专用的 ASIC 芯片主要起到加速防火墙策略检查、加密、认证，以及 PKI 过程功能。例如，所有的规则都存储在一个特定的存储区里，当硬件引擎每次需要检查规则时，就去扫描存储区。因此，检查一条规则或 20 条以上的规则并不会使性能有什么重大的不同。

另一方面，为了使硬件和软件处理达到最佳配合，NetScreen 使用了高速的多总线体系结构，该体系结构中的每个 ASIC 芯片都配有一个 RSIC 处理器、SDRAM 和以太网接口。因此，NetScreen 特有的硬件体系结构的设计比使用公共的 PC 硬件的防火墙产品性价比高。

（2）专用实时嵌入式操作系统。

NetScreen 使用专门的 ASIC 硬件设计之后，在操作系统也采用了专用的嵌入式操作系统——ScreenOS。在 NetScreen 防火墙中，每个 RISC 处理器都运行 ScreenOS。ScreenOS 是一个强安全，低维护费用，专门为 ASIC 线路设计的实时嵌入式操作系统。ScreenOS 的任务主要有三方面。首先，ScreenOS 支持从 WebUI（Web 界面）和 CLI（用户界面）获取配置，管理和监控任务。其次，ScreenOS 和高性能的 TCP/IP 引擎集成并与 ASIC 芯片紧密合作完成包的检测和转发的功能。最后，由于 ScreenOS 不像其他公用的操作系统平台受到连接表和处理数目的限制，因此一般 ScreenOS 每秒能支持的 TCP 并发连接数可达到 19 600 个。

NetScreen 专用 ASIC 硬件和专用 ScreenOS 操作系统如何配合，才能在对安全策略的处

理方面达到高性能？NetScreen 对包的检测主要分如下几个步骤：首先，进来的包在网络层被拦截，ScreenOS 提供包的格式和框架的检查，以辨认是否是畸形包。其次，如果包是合法的，ScreenOS 将检查该包是否属于存在的 TCP 会话。再次，如果该包所属的 TCP 会话的确存在，那么 ScreenOS 将检查 TCP 包的序列号和代码域，证明包真正属于该会话。如果该包不属于一个已存在的 TCP 会话，那么 ASIC 芯片要检测该包是否符合安全策略，如果不符合安全策略，则丢包，否则建立新的连接通信。NetScreen 防火墙对包的处理过程如图 4-2 所示。

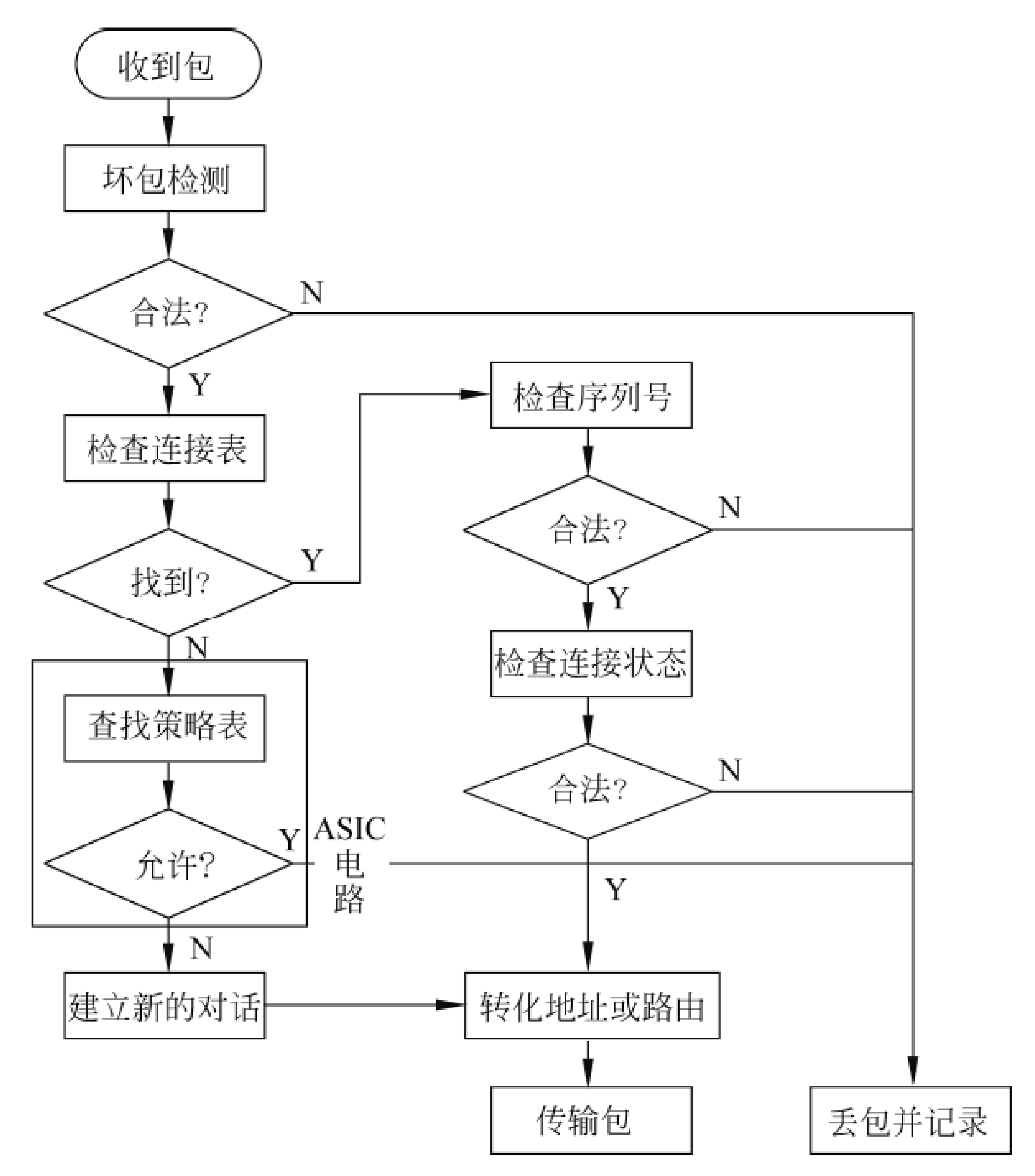


图 4-2　NetScreen 防火墙对包的处理过程

（3）多 CPU 和大容量 RAM。

除使用专用的硬件和软件设计，大多数的硬件防火墙都采用通用 PC 系统和通用的操作系统，如 linux、Solaris、Windows 等。这些厂家为了提高整体硬件的性能，一般增加参加并行处理的 CPU 数目以及 RAM 的容量。CyberGuard 防火墙就是一个典型的例子，该防火墙使用的 CPU 数达到 4 个，而 RAM 的容量为 1GB。

（4）检测算法改进。

前面都是从硬件和操作系统方面提高防火墙的性能，另一个提高防火墙的方法则是从数据包的检测方法上提高性能。以下是由几种典型的包检测的改进方法。

首先，就是前面提到的全状态检测。Checkpoint Firewall-1 的检测模块的工作都在操作系统的内核完成，它可以检测所有七层通信协议，并且可以分析包的状态信息。因此既能保证包检测的性能，又能保证包检测的全面性。之所以 Firewall-1 检测模块能做到检测应用层，是因为 Firewall-1 对 IP 包的内部结构很清楚，因此检测模块可以从包的应用内容中提取数据并将其保存下来，为后面的包提供必要的状态信息。Firewall-1 检测模块的工作原理

图如图 4-3 所示。

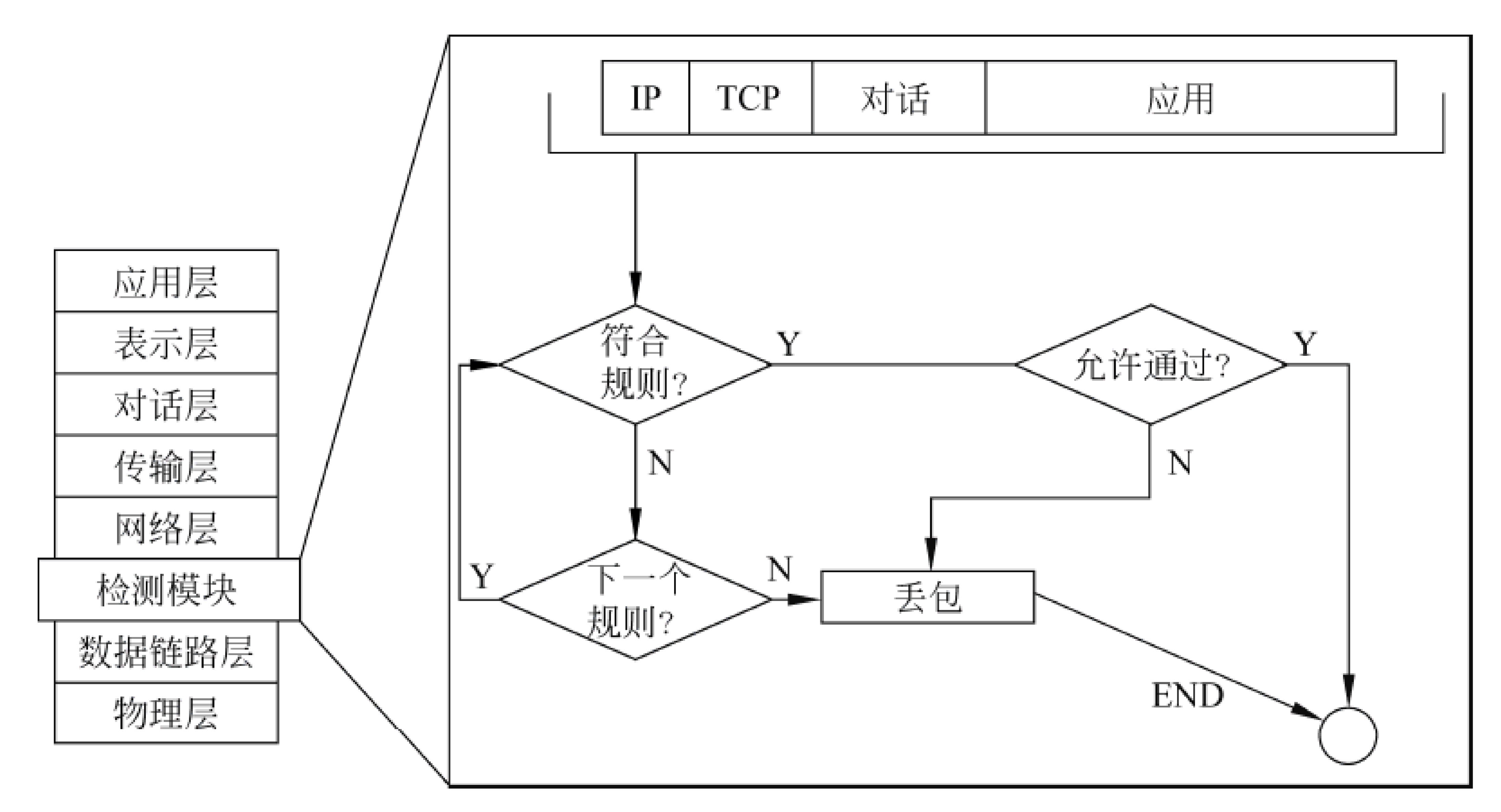


图 4-3　Firewall-1 检测模块的工作原理图

其次，就是自适应代理。自从 Network　Associates 的防火墙使用了自适应代理体系结构，由于只在防火墙检测到可疑通信量时才启用代理，因此在启用 NAT 后，Gaunlet 防火墙的性能比 NetScreen 和 Checkpoint 甚至更好。由于在 NetWork Associates 中找不到更多的关于自适应代理的资料，因此对自适应代理基本原理的描述只局限于前面提到的一部分。

再次，是 MAC 层状态检测。这是 NetGuard 公司为其防火墙提出的一种检测方法，由于包的检测处于 MAC 层，因此能很明显地提高防火墙的性能，并且使得它对操作系统安全漏洞具有免疫功能。

最后，快速代理（cut-through proxy）。这是由 Cisco 公司对代理性能的一种改进，但是这种改进是否安全还须考证。Cisco 认为一个代理服务器必须对包进行七层协议的检查是很浪费时间的，而 PIX 防火墙只是对每个通信连接的开始通过认证服务器进行必要的用户认证（如外部用户采用一次性口令），然后就可建立起直接的数据流，这样速度自然要快得多。Cisco 在检测安全时还使用了适应性安全算法（adaptive security algorithm），该算法接近状态检测，它将防火墙连接的网络进行安全分级，ASA 算法遵守下列规则：每个包必须经过状态检查；除了被安全策略拒绝，任何从安全区域向相对不安全区域发的包放行；除了被安全策略允许，任何从相对不安全区域向安全区域发的包拒绝；所有 ICMP 包除被指定允许外，都拒绝。从 Cisco 提出的 ASA 算法和 cut-through proxy 的方案可以看出，Cisco 是想通过牺牲安全度来换取性能。

（二）功能实现

防火墙的功能多种多样，国外各个厂家一方面都提供了一些防火墙基本功能和常见功能，另一方面也有自己的一些特色功能。防火墙的基本功能和常见的功能（如 NAT、PAT、内容过滤、负载平衡、高可靠性、透明模式等网盾防火墙）已基本实现，下面对未常见的一些功能进行简单描述。

（1）多种身份认证体系和灵活的认证方法。

由于现今各种操作系统都支持多种认证方案，因此许多防火墙厂商为用户提供了多种认证体系，以便用户使用。例如，Checkpoint 认证体系大概有 7 种：防火墙口令、RADIUS

或 TACACS/TACACS+服务器、数字证书、S/Key、SecurID Tokens、Axent Pathways Defender、OS 口令。

为了使防火墙用户能灵活地控制认证对象，Checkpoint 还提供了 3 种不同的认证方法：用户认证、IP 地址认证、对话认证（基于每个对话对每个服务作认证）。

最后一个是许多公司提出的透明的用户 ID 和地址认证服务体系。该种透明认证的实现是通过将 Windows NT 的域认证方案和它的防火墙合为一体。该透明的认证服务可以自动捕捉 Windows NT 系统的登录信息和本机动态分配的地址，然后这些捕捉到的信息就可以直接作为防火墙认证的信息，这样就可以做到用户透明认证。

（2）防病毒检测。

很多防火墙都增加了防病毒功能，一般是通过集成第三方的防病毒软件实现的，例如，Checkpoint 通过它的 CVP（Content Vectoring Protocol）服务器集成第三方的防病毒产品。如果防火墙的 FTP 服务需要病毒检测，那么防火墙就会拦截 FTP 传送的文件送往 CVP 服务器接受检测，然后防火墙再根据 CVP 服务器的检查处理该 FTP 的连接。

（3）入侵检测。

在防火墙中绑定入侵检测也是现在国外增强防火墙安全性的一种重要方法。防火墙对安全的手段一般趋于静态，而入侵检测则趋于动态，对安全的防范做到动静结合是很多厂家的想法。但是，做到入侵检测和防火墙真正紧密配合还是要花一定的功夫。例如，入侵检测是否可以根据检测到的情况直接对防火墙进行动态控制？

（4）多媒体服务支持。

互联网的多媒体应用在企业和用户中已经很流行了，但是多媒体应用由于要求打开许多端口，也给网络安全带来一定的威胁。由于多媒体应用的一个重要特征是数据量大而且要求速度快，因此对付防火墙的安全性检查的性能就需要一定的要求，Cisco 公司的产品 PIX 对多媒体应用很重视，他自称可以做到性能和安全兼得。他们支持的多媒体应用包括 RealAudio、Streamworks、CU-SeeMe、Internet Phone、IRC、Vxtreme、VDO Live。

（5）VPN。

VPN 是指在公共通信通道中使用虚拟隧道的技术，由于这种应用的客户需求很大，因此几乎所有的防火墙厂家都将它与防火墙绑定。他们都将管理简易、高速吞吐量和强有力的安全特性作为衡量 VPN 好坏的标准。

CommWeb 和 Network Test Inc 进行合作测试，最后发现有 3 个网关能够提供安全性、可扩展性、使用简单和价格性能比的最佳组合。具有最高水平的设备是来自 NetScreen Technologies Inc 的 NetScreen-100，它没有安全问题，在我们测试的任何设备中都具有最高的吞吐量，同时有一个比较公平的价格。来自 Cisco Systems Inc 的 Cisco 7100 VPN 路由器和其他测试设备相比，提供更加强大的安全性能，具有优秀的管理特点，同时支持更多的并发连接，尽管其价格高了一些。Lucent Technologies 的 VPN Firewall Brick 80 在我们测试的高端设备中提供非常好的管理性能、极佳的参数和最好的性价比。

（三）管理

防火墙的功能和性能固然重要，但是系统管理员是通过防火墙的管理界面控制防火墙的，提供一个系统、灵活、简单且直观的管理也是防火墙吸引客户的一个重要方面。因此，

国外的厂家在管理界面方面也下了一定功夫，成为他们宣传中的一个亮点。

（1）基于客户机/服务器的管理方式。

Checkpoint 的管理具有它的独特性，而且它的管理方式在业界享有盛誉，因此给我留下很深的印象。Checkpoint 的管理模式是基于客户机/服务器方式的，如图 4-4 所示。这种管理方式具有高性能、可扩展、集中管理等优点。在这种模式下，管理员可以通过单一的用户界面对公司中的网络安全设备进行配置、管理和监控。这种管理模式由三部分组成：用户界面（GUI）、管理服务器、网络安全模块。其中，管理服务器相当于安全数据库，它储存了网络对象定义、用户定义、安全策略、所有网络安全设备的日志文件等信息。然后，管理服务器将这些安全策略下载到各网络安全设备。还有各个安全设备的升级问题也可以由管理服务器统一管理，只要更新管理服务器上的版本，需要更新的安全设备就会觉察到这种改变接着从管理服务器上下载更新文件自动更新自己。

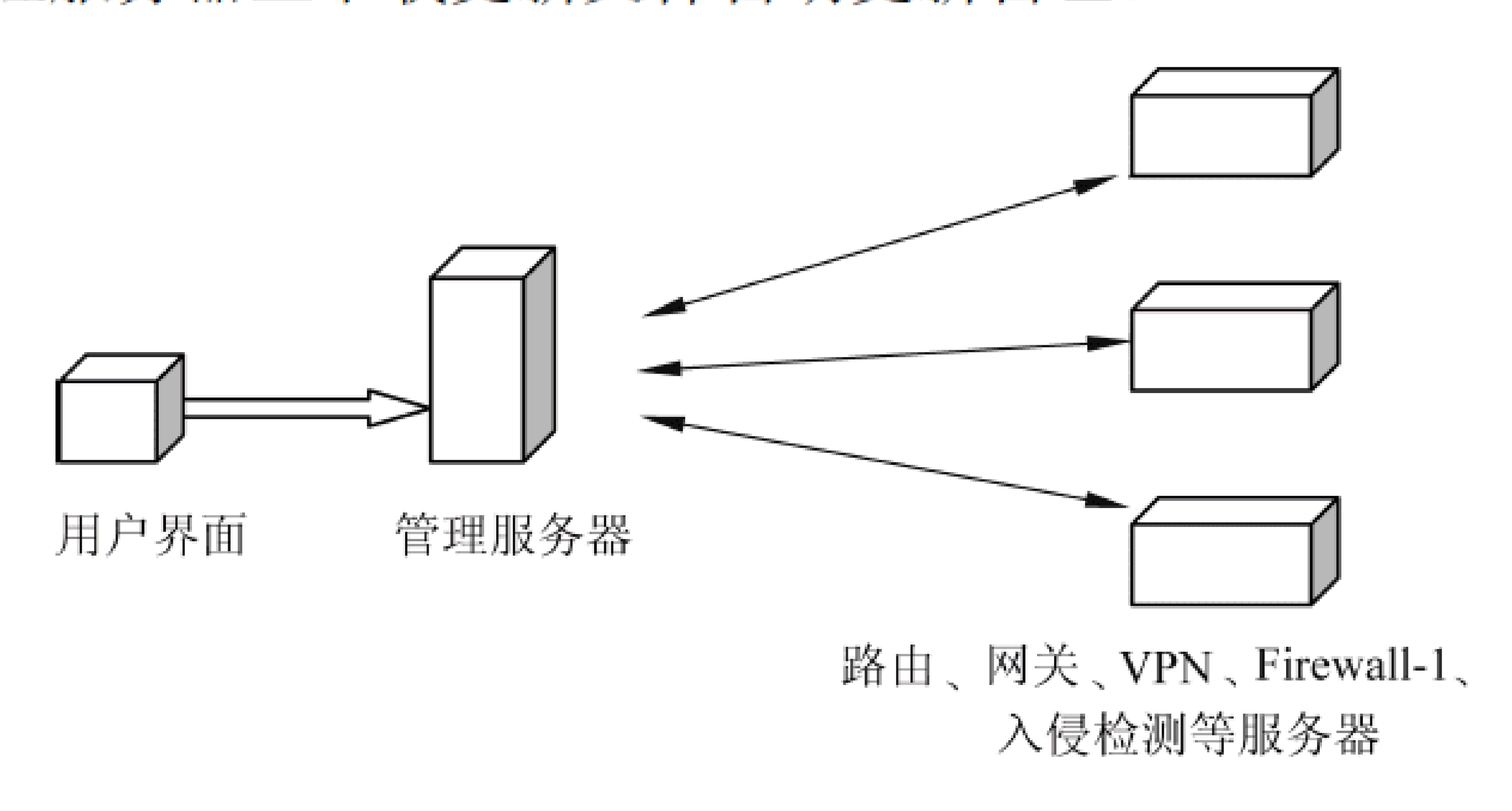


图 4-4　分布式客户/服务器管理模式

（2）简单的面向对象管理思想。

Checkpoint 对安全策略的配置是基于面向对象思想的。他们把网络资源（网段、路由器、网关、服务）看作是一个对象，这些对象都有一套各自的属性，如姓名、IP 地址或范围、NAT 等。然后，定义好的对象就可以在规则策略表（rule base）中方便地使用。因此，为整个网络通信定义的规则策略表显得非常简练、清楚。该规则表的原型可以在 Firewall-1 的 demo 中看到。

（3）视觉化策略编辑。

为了使管理员对整个网络的结构有一个直观的理解，Checkpoint 的界面使网管者可以检视图形化的整体网路安全部署架构，同时管理安全政策。「视觉化策略编辑」会显示进入企业网路的连线，而任何安全政策的改变都会显示在「视觉化策略编辑」的图示中，以真实反映网路安全的状况，同时确保较高等级的安全。

（4）多种管理方式。

由于管理员控制设备的习惯各异，而且配置过程中实际情况不同，因此为管理员准备多种配置方式很有必要。基本方式有带 Web 服务器，方便地通过流行的浏览器进行管理；Windows 95/NT/2000 图形界面：可关闭远程的管理方式，只用本地的安全的管理；SNMP 管理方式：通过网络管理软件管理；命令行界面：支持批处理方式及通过调制解调器的备用渠道进行控制。

10. 浏览最热门的 3 个防火墙技术网站，综述目前关于防火墙讨论的热点问题。

答：下一代防火墙（NGFW）网址：

（1）Cisco。

https://www.cisco.com/c/zh_cn/products/security/firewalls/index.html?ccid=cc000291&dtid=psebdu000857&oid=0&POSITION=SEM&COUNTRY_SITE=cn&CAMPAIGN=sc-06&CREATIVE=CN_SEM_SEC_Fire-AO_PM_NB-Fire%7cAO_psebdu000857_cc000291_0&REFERRING_SITE=Baidu&KEYWORD=%E9%98%B2%E7%81%AB%E5%A2%99&dclid=COPLhfGGhNsCFcgNKgod4l0IBA；

热点问题：下一代防火墙的 5 个选择技巧，针对高级攻击的高级防御，应用可视性和可控性，下一代防火墙资源中心。

（2）深信服科技。

http://www.sangfor.com.cn/product/safety-perimeter-security-af.html?utm_source=baidu&utm_medium=PC&utm_campaign=03_pc_%CF%C2%D2%BB%B4%FA%B7%C0%BB%F0%C7%BDAF_%C8%AB%B9%FA_D&utm_content=AF-%BA%CB%D0%C4%B4%CA&utm_term=%B7%C0%BB%F0%C7%BD%D3%B2%BC%FE

热点问题：未知威胁检测，威胁情报，安全云。

（3）https://comodo.cn/科摩多。

热点问题：Korugan 统一威胁管理，一站式网络和终端保护的 Korugan 统一威胁管理设备，使用 BIND DNS 关键更新，互联网系统协会（ISC）已经发布了安全更新，以解决多个 BIND 的漏洞，移动设备管理器 3.0。

11. 有一个内部网（192.168.20.0）只与某一台外部主机（172.1652.55）交换数据。写出位于它们之间的数据包过滤规则。

答：只允许源或目的 IP 地址为 172.165.2.55 的数据包通过。

12. 比较包过滤、网络地址转换和代理技术的特点以及适用的环境。

答：（1）数据包过滤技术的特点：

数据包过滤器工作在网络的底层（IP 层），在网络中适当的位置上对数据包实施有选择的过滤。当数据包通过时，过滤系统（路由器、网桥或单独的主机）将检查数据包的 IP 头和 TCP 头或 UDP 头，根据既定原则决定是否允许数据包通过。数据包过滤的工作原理如图 4-5 所示。

按源地址进行过滤是最简单的数据包过滤方式。防火墙只检查数据包的目标地址和源地址，根据规则决定是否允许该包通过。采用这种方式的典型产品有美国 Cisco 公司提供的防火墙。采用基于路由器的包过滤器作为防火墙，可以提供廉价、有效并具有一定网络安全的环境。它对用户提供服务透明，用户不用改变客户端程序或自己的行为。它处理包的速度是最快的，但提供的安全级别低，而且相对代理服务有内在的缺点，如维护困难；不能防止某些 IP 地址欺骗（如外部主机伪装其他外部主机的 IP）；不能提供有用的日志，以追踪入侵者；不能屏蔽网络内部结构。

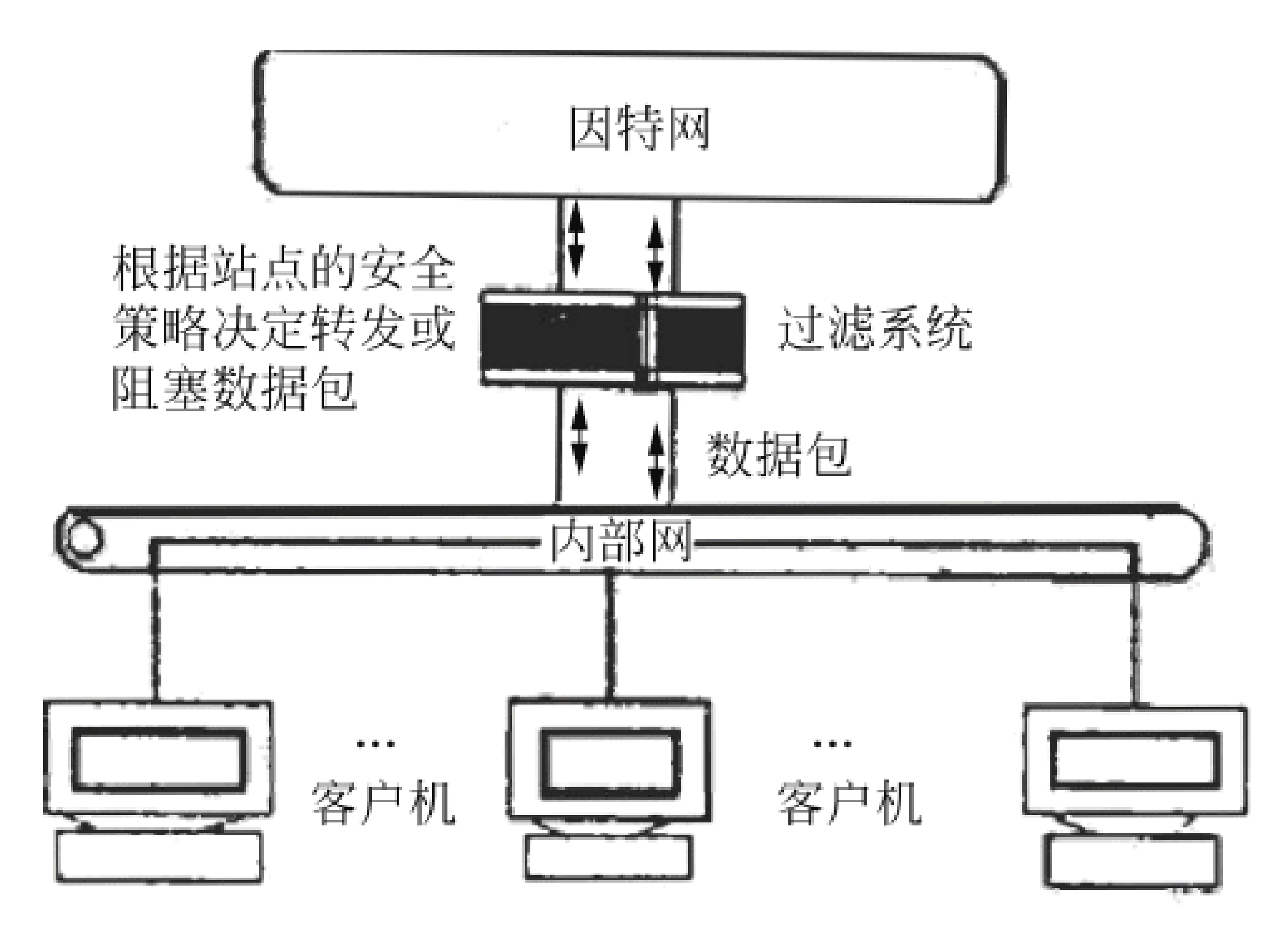


图 4-5　数据包过滤的工作原理

目前，我国多数学校的校园网是通过 Cisco 路由器与 CERNET 相连的。Cisco 公司基于包过滤的路由器采用两种方法实现防火墙功能：一种是适用于某些接口上的流控制，用于过滤 IP 或指定 TCP 和 UCP 端口的 IP 数据包；另一种是适用于广播信息，用于过滤广播信息。由于校园网的 IP 地址范围是确定的，拥有明确的闭合边界，较易进行地址控制；而作为一种较具开放性的学术环境，它受到入侵的威胁也相对较小，因此采用数据包过滤这种代价较小的防火墙目前是可行的。

（2）网络地址转换——电路级网关技术的特点。

电路级网关用来监控受信任的客户或服务器与不受信任的主机间的 TCP 握手信息，决定该会话是否合法，它工作在会话层中。使用 TCP 首先必须通过三次握手建立 TCP 连接，然后才开始传送数据。电路级网关通过检查在 TCP 握手过程中双方的 SYN、ACK 和序列数据是否为合理逻辑，来判断该请求的会话是否合法。如果该网关认为会话是合法的，就会为双方建立连接，之后网关仅转发数据，而不进行过滤。电路级网关通常需要依靠特殊的应用程序完成复制传递数据的服务。电路级网关是一个通用代理服务器，它工作于 OSI 互联模型的会话层或 TCP/IP 的 TCP 层。它适用于多个协议，但它不能识别在同一个协议栈上运行的不同的应用，当然也就不需要对不同的应用设置不同的代理模块。电路级网关还提供一个重要的安全功能：网络地址转换（NAT），将所有的内部 IP 地址都映射到防火墙使用的一个“安全”的 IP 地址，使得传递的数据似乎起源于防火墙，从而隐藏了被保护网络的信息。

实际上，电路级网关并非作为一个独立的产品存在，它通常与其他的应用级网关结合在一起，所以有人也把电路级网关归为应用级网关，但它在会话层上过滤数据包，无法检查应用层级的数据包，适用于小型局域网。

（3）代理服务防火墙技术的特点。

代理服务是运行在防火墙上的一种服务器程序。典型的代理接受用户的客户请求，先判断用户和用户的 IP 地址是否有权使用代理服务器（也可能支持其他的认证手段），然后代表客户与真实服务器之间建立连接。其典型产品是美国网络联盟（NAI）的 Gauntlet。代理系统是客户机和真实服务器之间的中介，代理系统完全控制客户机和真实服务器之间的流量，并对流量情况加以记录。它一般工作在双重宿主主机（有两个网络接口的计算机系统）或堡垒主机上，是这些系统的核心。

代理服务器是防火墙技术中颇受推崇的一种技术，它能提供比包过滤技术更安全的保护。其优点是：可以屏蔽网络内部结构，增强网络的安全性，同时还可用于实施数据流监控、过滤、记录、报告等功能。使用代理服务器的缺点是对用户不透明，且由于代理服务器具有相当大的工作量，通常需要高性能服务器承担，故其总体投资也相对较高，适用于企业环境。

13. 简述国内外物理隔离技术的现状和发展趋势。

答：国家保密局 2000 年 1 月 1 日起颁布实施的《计算机信息系统国际联网保密管理规定》中规定："涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其他公共信息网络相连接，必须实行物理隔离"，物理隔离安全技术采用硬件物理隔离方案，将内部涉密网与外部网彻底地物理隔离开，没有任何线路连接。这样可以保证网上黑客无法连接内部涉密网，具有极高的安全性，但也可能造成工作不便、数据交流困难、设备场地增加和维护费用提高等负面影响。尽管如此，瑕不掩瑜，物理隔离仍是目前保障信息安全的有效措施。

目前，物理隔离技术现状如下。

（1）物理隔离在安全上的要求主要概括为两点。

其一，在物理传导上使涉密网络和公共网络隔断，确保公共网络不能通过网络连接而侵入涉密网络，同时防止涉密网络信息通过网络连接泄露到公共网络。

其二，在物理储存上隔断涉密网络和公共网络，对于断电后会遗失信息的部件，如内存、处理器等暂存部件，要在网络转换时作清除处理，防止残留信息泄露；对于断电后信息非遗失性设备（如磁带机、硬盘等存储设备），涉密网络与公共网络信息要分开存储。

（2）物理隔离的分类。

当前的网络物理隔离主要在如下几个方面作防护。

A. 客户端的物理隔离

现在应用最多的是客户端的物理隔离方案，这种方案用于解决网络的客户端的信息安全问题，假定某机构的网络已经分为两个网络，一个是内部涉密网，一个是外部公共网，内部涉密网用于工作于安全的涉密环境，不与外部网络有任何连接；外部公共网则是开放的，可以连接 Internet 发布信息。在网络的客户端应用物理隔离卡产品可以使一台工作站计算机既可以连接内部网，又可以连接外部网，可在内外网上分时工作，同时绝对保证内外网之间物理隔离，达到了方便工作、节约资源的目的。

B. 集线器级的物理隔离

集线器级的物理隔离产品需要与客户端的物理隔离产品结合起来应用，可以在客户端的内外双网的布线上使用一条网络线通过远端切换器连接内外双网，实现一台工作站连接内外两个网络的目的，并在网络部线上避免了客户端计算机要用两条网络线连接网络。

C. 服务器端的物理隔离

服务器端的物理隔离产品是一种崭新的高级隔离产品，现在一些国外的产品已经应用，但国内还没有较好的产品，它通过复杂的软硬件技术实现在服务器端的数据过滤和传输任务，其技术关键还是在同一时刻内外网络没有物理上的数据连通，但又快速分时地处理并

传递数据。

（3）如何实现物理隔离。

目前，网络隔离技术有如下两种。

① 单主板安全隔离计算机：其核心技术是双硬盘技术，将内外网络转换功能写入BIOS中，并将插槽也分为内网和外网，使用更方便，也更安全。

单主板安全隔离计算机是采用彻底实现内外网物理隔离的个人计算机，这种安全计算机的成本仅增加了25%左右，并且由于这种安全计算机是在较低层的BIOS上开发的，处理器、主板、外设的升级不会给计算机带来“不兼容”的影响。它很好地解决了接入网络后局域网络信息安全、系统安全、操作安全和环境安全等问题，彻底实现了网络物理隔离。

安全计算机在传统PC主板结构上形成了两个物理隔离的网络终端接入环境，分别对应于国际互联网和内部局域网，保证局域网信息不会被互联网上的黑客和病毒破坏。主板BIOS控制由网卡和硬盘构成的网络接入和信息存储环境各自独立，并只能在相应的网络环境下工作，不可能在一种网络环境下使用另一环境才使用的设备。BIOS还提供所有涉及信息发送和输出设备的控制，包括：

（a）对软驱、光驱提供限制功能。在系统引导时不允许驱动器中有移动存储介质。双网计算机提供软驱关闭/禁用功能。

（b）对双向端口设备提供限制功能。双向端口包括打印机并行接口、串行接口、USB接口、MIDI接口，这些接口如果使用不当，也是安全漏洞，需要加强使用管制。对于BIOS，则由防写跳线防止病毒破坏、非法刷新或破坏，以及改变BIOS的控制特性。

② 网络安全隔离卡：其核心技术是双硬盘技术，启动外网时关闭内网硬盘，启动内网时关闭外网硬盘，使两个网络和硬盘物理隔离，它不仅可用于两个物理隔离的情况，也可用于个人资料要保密又要上互联网的个人计算机的情况。其优点是价格低，但使用稍麻烦，因为转换内外网要关机和重新开机。

网络安全隔离卡的功能是以物理方式将一台PC虚拟为两部计算机，实现工作站的双重状态，既可在安全状态，又可在公共状态，两种状态是完全隔离的，从而使一部工作站可在完全安全状态下连接内外网。网络安全隔离卡实际是被设置在PC中最低的物理层上，通过卡上一边的IDE总线连接主板，另一边连接IDE硬盘，内、外网的连接均须通过网络安全隔离卡，PC硬盘被物理分隔为两个区域，在IDE总线物理层上，在固件中控制磁盘通道，任何时候数据只能通过一个分区。

在安全状态时，主机只能使用硬盘的安全区与内部网连接，而此时外部网（如Internet）连接是断开的，且硬盘的公共区的通道是封闭的；在公共状态时，主机只能使用硬盘的公共区与外部网连接，而此时与内部网是断开的，且硬盘安全区也是被封闭的。

当两种状态转换时，可通过鼠标单击操作系统上的切换键，进入一个热启动过程。切换时，系统通过硬件重启信号重新启动，这样，PC内存的所有数据就被消除，两个状态分别是有独立的操作系统，并独立导入，两种硬盘分区不会同时激活。为了保证安全，两个分区不能直接交换数据，但是用户可以通过一个独特的设计，安全方便地实现数据交换，即在两个分区外，网络安全隔离在硬盘上另外设置了一个功能区，该功能区在PC处于不同的状态下转换，即在两种状态下功能区均表现为硬盘的D盘，各个分区可以通过功能区作

为一个过渡区交换数据。当然，根据用户需要，也可创建单向的安全通道，即数据只能从公共区向安全区转移，但不能逆向转移，从而保证安全区的数据安全。

14. 浏览网站，列举国内有关物理隔离设备的厂家及其产品的特点。

答：Tenix 的产品 Interactive Link 具有将私有网络与公网彻底隔离，限定网络流量的单向性，故称之为数据二极管，网址为 http://www.tenixdatagate.com/Main.asp?ID=880。

15. 收集国内外有关网络隔离技术的网站信息，简要说明各网站的特点。

答：略

16. 收集国内外有关网络隔离技术的最新动态。

答：面对新型网络攻击手段的出现和高安全度网络对安全的特殊需求，全新安全防护防范理念的网络安全技术——“网络隔离技术”应运而生。网络隔离技术的目标是确保隔离有害的攻击，在可信网络之外和保证可信网络内部信息不外泄的前提下，完成网间数据的安全交换。网络隔离技术是在原有安全技术的基础上发展起来的，它弥补了原有安全技术的不足，突出了自己的优势。网络隔离的英文名为 Network Isolation，主要是指把两个或两个以上可路由的网络（如 TCP/IP）通过不可路由的协议（如 IPX/SPX、NetBEUI 等）进行数据交换而达到隔离目的。由于其原理主要是采用了不同的协议，所以通常也称协议隔离（protocol isolation）。1997 年，信息安全专家 Mark Joseph Edwards 在他编写的一书中，就对协议隔离进行了归类。在书中他明确指出协议隔离和防火墙不属于同类产品。隔离概念是在为了保护高安全度网络环境的情况下产生的；隔离产品的大量出现也是经历了五代隔离技术不断的实践和理论相结合后得来的。

第一代隔离技术——完全的隔离。此方法使得网络处于信息孤岛状态，做到了完全的物理隔离，需要至少两套网络和系统，更重要的是信息交流的不便和成本的提高，这样给维护和使用带来了极大的不便。

第二代隔离技术——硬件卡隔离。在客户端增加一块硬件卡，客户端硬盘或其他存储设备首先连接到该卡，然后再转接到主板上，通过该卡能控制客户端硬盘或其他存储设备。而在选择不同的硬盘时，同时选择了该卡上不同的网络接口，连接到不同的网络。但是，这种隔离产品有的仍然需要网络布线为双网线结构，产品存在着较大的安全隐患。

第三代隔离技术——数据转播隔离。利用转播系统分时复制文件的途径实现隔离，切换时间非常久，甚至需要手工完成，不仅明显地减缓了访问速度，更不支持常见的网络应用，失去了网络存在的意义。

第四代隔离技术——空气开关隔离。它是通过使用单刀双掷开关，使得内外部网络分时访问临时缓存器完成数据交换的，但在安全和性能上存在许多问题。

第五代隔离技术——安全通道隔离。此技术通过专用通信硬件和专有安全协议等安全机制，实现内外部网络的隔离和数据交换，不仅解决了以前隔离技术存在的问题，并有效地把内外部网络隔离开来，而且高效地实现了内外网数据的安全交换，透明支持多种网络应用，成为当前隔离技术的发展方向。

17. 简述 VPN 使用了哪些主要技术。

答：（1）MPLS VPN 是一种基于 MPLS 技术的 IP VPN，是在网络路由和交换设备上应用多协议标记交换（Multiprotocol Label Switching，MPLS）技术，简化核心路由器的路由选择方式，利用结合传统路由技术的标记交换实现的 IP 虚拟专用网络（IP VPN）。MPLS 的优势在于将二层交换和三层路由技术结合起来，在解决 VPN、服务分类和流量工程这些 IP 网络的重大问题时具有很优异的表现。因此，MPLS VPN 在解决企业互连、提供各种新业务方面也越来越被运营商看好，成为在 IP 网络运营商提供增值业务的重要手段。MPLS VPN 又可分为二层 MPLS VPN（即 MPLS L2 VPN）和三层 MPLS VPN（即 MPLS L3 VPN）。

（2）SSL VPN 是以 HTTPS（Secure HTTP，安全的 HTTP，即支持 SSL 的 HTTP）为基础的 VPN 技术，工作在传输层和应用层之间。SSL VPN 充分利用了 SSL 协议提供的基于证书的身份认证、数据加密和消息完整性验证机制，可以为应用层之间的通信建立安全连接。SSL VPN 广泛应用于基于 Web 的远程安全接入，为用户远程访问公司内部网络提供了安全保证。

（3）IPSec VPN 是基于 IPSec 协议的 VPN 技术，由 IPSec 协议提供隧道安全保障。IPSec 是一种由 IETF 设计的端到端的确保基于 IP 通信的数据安全性的机制。它为 Internet 上传输的数据提供了高质量的、可互操作的、基于密码学的安全保证。

18. 综述有关入侵检测技术的各种定义。

答：入侵检测是用来发现外部攻击与内部合法用户滥用特权的一种方法，是一种动态的网络安全技术。它利用各种不同类型的引擎，实时或定期地对网络中相关的数据源进行分析，根据引擎对特殊数据或事件的认识，将其中具有威胁性的部分提取出来，并触发响应机制。其动态性反映在入侵检测的实时性和对网络环境的变化具有一定程度上的自适应性，这是以往静态安全技术无法具有的。入侵检测技术作为一种主动防御技术，是信息安全技术的重要组成部分，是传统计算机安全机制的重要补充。

入侵检测系统就是一种利用入侵检测技术对潜在的入侵行为做出记录和预测的智能化、自动化的软件或硬件系统。

入侵检测系统的一般组成主要有采集模块、分析模块和管理模块。采集模块主要用来搜集原始数据信息，将各类混杂的信息按一定的格式进行格式化并交给分析模块分析；分析模块是入侵检测系统的核心部件，它完成对数据的解析，给出怀疑值或做出判断；管理模块的主要功能是根据分析模块的结果做出决策和响应。管理模块与采集模块一样，分布于网络中。为了更好地完成入侵检测系统的功能，系统一般还有数据预处理模块、通信模块和数据存储模块等。

根据数据来源的不同，入侵检测系统常被分为基于主机（Host-based）的入侵检测系统和基于网络（Network-based）的入侵检测系统。

19. 入侵检测系统有哪些可以利用的数据源？

答：主机和网络。基于主机的入侵检测系统的数据源来自主机信息，如日志文件、审

计记录等。基于主机的入侵检测系统的检测范围较小，只限于一台主机内。它不但可以检测出系统的远程入侵，还可以检测出本地入侵，但由于主机的信息多种多样，对于不同的操作系统，信息源的格式就不同，这使得基于主机的入侵检测系统比较难实现。

随着计算机网络技术的发展，单独依靠主机审计信息进行入侵检测难以适应网络安全的需求，于是人们提出了基于网络的入侵检测系统体系结构，这种检测系统根据网络流量、单台或多台主机的审计数据检测入侵。

基于网络的入侵检测系统的数据源是网络流量，它实时监视并分析通过网络的所有通信业务，检测范围是整个网络，由于网络数据是规范的 TCP/IP 数据包，所以基于网络的入侵检测系统比较易于实现，但它只能检测出远程入侵，对于本地入侵，它是看不到的。

20. 试构造一个网络数据包的截获程序。

答：程序构造思路：网卡层面的截获（截获和自己同网段的计算机发送的信息，包括送往自己的数据包）。

一个网络数据报文的发送过程是这样的：

a. 发送方的应用层将要发送的数据报文，通过 Socket 调用提交 TCP/IP 层。

b. TCP/IP 层经过层层封装，将这些数据报文封装成 IP 数据报文，送往数据链路层，一般以太网用的是 802.x 的帧结构，封装成数据帧。

c. 以太网数据链路层是使用 MAC 地址标识网口的，每一网口的 MAC 地址都是世界唯一的。

d. 数据链路层将目的方的MAC地址和自己的MAC地址分别填入目标MAC和源MAC的字段中，发送到物理层（也就是网线上）。

网络数据报文的接收过程：

每个网卡在收到物理链路上发送来的数据帧之后，都会自动检测收到的这个 MAC 地址是否和自己的网卡 MAC 地址相同，如果相同，则接受，否则就丢弃。

这样就可以实现对于数据包的过滤过程。而很多网络拦截工具，如 Sniffer 或者 Ethereal，都将网卡的这个功能打破。他们定义了一个网卡所谓的混杂模式，这里，网卡不管收到的这个数据包是否是给自己的（目的 MAC 和自己网卡的 MAC 是否相同），都往上层送，都能对数据流进行分析。这就是网络层面拦截的基本原理。

21. 试述入侵检测系统的工作原理。

答：入侵检测是用来发现外部攻击与内部合法用户滥用特权的一种方法，是一种动态的网络安全技术。它利用各种不同类型的引擎，实时或定期地对网络中相关的数据源进行分析，根据引擎对特殊数据或事件的认识，将其中具有威胁性的部分提取出来，并触发响应机制。其动态性反映在入侵检测的实时性、对网络环境的变化具有一定程度上的自适应性，这是以往静态安全技术无法具有的。入侵检测技术作为一种主动防御技术，是信息安全技术的重要组成部分，是传统计算机安全机制的重要补充。

入侵检测系统就是一种利用入侵检测技术对潜在的入侵行为做出记录和预测的智能化、自动化的软件或硬件系统。

22. 收集资料，对国内外主要基于网络的入侵检测产品进行比较。

答：（1）Snort。Snort 是一个免费、开放源代码的基于网络的入侵检测系统。它具有很好的配置性和可移植性。

Snort 最初是设计给小网络段使用的，常被称为轻量级的入侵检测系统。现在，Snort 既可用于 UNIX/Linux 平台，也有适用于 Windows 操作系统的版本，并且已经有了方便的图形用户界面。

扩展性很好：基于规则的体系结构使 Snort 非常灵活，设计者使其很容易插入和扩充新的规则——就能对抗新出现的威胁。

Snort 具有实时数据流量分析和日志 IP 网络数据包的能力，能截获网络中的数据包并记录数据包日志。日志格式既可以是 Tcpdump 式的二进制格式，也可以解码成 ASCII 字符形式，还可以通过数据库输出插件记入数据库。

Snort 能够对多种协议进行协议解析，对内容进行搜索和匹配。它能够检测多种方式的攻击和探测。

（2）ISS RealSecure。Internet Security System 公司的 RealSecure 是一种实时监控的软件，它由控制台、网络引擎和系统代理三部分组成。网络引擎基于 C 类网段，安装在一台单独使用的计算机上，通过捕捉网段上的数据包，分析包头和数据段内容，与模板中定义的事件手法进行匹配，发现攻击后采取相应的安全动作。

系统代理基于主机，安装在受保护的主机上，通过捕捉访问主机的数据包，分析包头和数据段内容，与模板中定义的事件手法进行匹配，发现攻击后采取相应的安全动作。

控制台是安全管理员的管理界面，它可同时与多个网络引擎和系统代理连接，实时获取安全信息。

（3）Watcher。Watcher 是一个典型的网络入侵检测工具，它能检测所有通过网络的信息包，并且将它们当成恶意的攻击行为记录在 sys log 中，网络管理员根据记录下的日志可以分析、判断系统是否正在遭受恶意攻击。它是一个完全免费的版本，安装起来非常简单。

23. 收集资料，对国内外主要基于主机的入侵检测产品进行比较。

答：常用的 HIPS 软件有 OSSEC HIDS，项目主页为 http://www.ossec.net，支持 Linux 和 Windows 系统，监测文件和目录修改；通过保存认证信息提供可说明性。但是，Server 要安装在 Linux 系统上。Agent 可以安装在 Linux 或者 Windows 上。

功能包括日志分析、rootkit 检测（不支持 Windows 系统）、完整性检测等。

当认证未通过或出现存在问题的用户添加时，触发用户报警，如 E-mail 报警、定时报警等。日志分析规则为 XML 格式，进程在 chroot jail 中运行并且权限隔离，遵守 syslog RFC 3164 协议。因为其强大的日志分析引擎，互联网供应商、大学和数据中心都乐意运行 OSSEC HIDS，以监视和分析其防火墙、IDS、Web 服务器和身份验证日志。

24. 分析入侵检测系统的不足和发展趋势。

答：入侵检测系统的不足在于：

（1）不能在没有用户参与的情况下对攻击行为展开调查。

（2）不能在没有用户参与的情况下阻止攻击行为的发生。

（3）不能克服网络协议方面的缺陷。

（4）不能克服设计原理方面的缺陷。

（5）响应不够及时，签名数据库更新得不够快。

（6）经常是事后才检测到，适时性不好。

随着网络攻击手段向分布式方向发展（如目前出现的分布 DoS 攻击），且采用了各种数据处理技术，其破坏性和隐蔽性也越来越强。相应地，入侵检测系统也在向分布式结构发展，采用分布收集信息、分布处理、多方协作的方式，将基于主机的 IDS 和基于网络的 IDS 结合起来使用，构筑面向大型网络的 IDS，而且对处理速度及各相关性能的要求更高。目前已有的 IDS 还远远不能满足入侵检测的需要。入侵检测技术的主要研究方向有：

（1）IDS 体系结构研究。IDS 是包括技术、人、工具三方面因素的一个整体，如何建立一个良好的体系结构，合理组织和管理各种实体，以杜绝在时间上和实体交互中产生的系统脆弱性，是当前 IDS 研究中的主要内容，也是保护系统安全的首要条件。

IDS 体系结构的研究主要包括：具有多系统的互操作性和重用性的通用入侵检测框架；总体结构和各部件的相互关系；系统安全策略；具有可伸缩性的统一 IDS 系统结构；IDS 管理；DARP 提出的通用入侵检测框架；具有可伸缩性、重用性的系统框架；安全、健壮和可扩展的安全策略。

（2）安全通信技术研究。目前，分布式系统的安全通信机制也是研究领域的一个热点，包括 IETF 的入侵检测报警协议（Intrusion Alert Protocol，IAP）、安全认证和远程控制等协议、高效且具有互操作性的安全通道。

（3）入侵检测技术研究。目前已有的入侵检测技术包括基于知识的检测和基于行为的检测。基于知识的检测包括专家系统、模型推理、状态转换图、信号分析、Petri Nets 图等。这种检测由于依据具体特征库进行判断，所以准确度很高、方便响应；但与具体系统依赖性太强，移植性不好，维护工作量大，受已有知识的限制，难以检测出权利滥用。基于行为的检测包括概率统计方法、神经网络方法、专家系统、用户意图识别、计算机免疫系统等。这种检测与系统相对无关，通用性较强；可检测出以前未出现过的攻击方法。它的主要缺陷在于误检率很高。

鉴于两者存在的优点和不足，而且已证明依靠单一的入侵检测方法不可能检测出所有入侵，所以现在的研究主要集中在对已有的检测方法进行改进和对新检测法的研究上，以期找到效率和效果相一致的检测方法。

（4）响应策略与恢复研究。IDS 识别出入侵后的响应策略是维护系统安全性、完整性的关键。IDS 的目标是实现实时响应和恢复。实现 IDS 的响应包括：向管理员和其他实体发出警报；进行紧急处理；对于攻击的追踪、诱导和反击；对于攻击源数据的聚集以及 ID 部件的自学习和改进。

IDS 的恢复研究包括：系统状态一致性检测、系统数据的备份、系统恢复策略和恢复时机。

（5）协作式入侵检测技术研究。随着黑客入侵手段的提高，尤其是分布式、协同式、

复杂模式攻击的出现和发展，传统的单一、缺乏协作的入侵检测技术已经不能满足需求，需要有充分的协作机制。协作主要包括两个方面：事件检测、分析和响应能力的协作；各部分掌握的安全相关信息的共享。尽管现在最好的商业产品和研究项目中也只有简单的协作，如 ISS 的 RealSecure 入侵检测产品可以与防火墙协作，AAFID 中同一主机上各主机型代理之间可进行简单的信息共享，但协作是一个重要的发展方向。协作的层次主要有以下几种：

同一系统中不同入侵检测部件之间的协作，尤其是主机型和网络型入侵检测部件之间的协作，以及异构平台部件的协作；不同安全工具之间的协作；不同厂家的安全产品之间的协作；不同组织之间预警能力和信息的协作。要实现协作，首先要考虑两个问题: 一是信息表达的格式和信息交换的安全协议；二是协作的模型。信息表达的格式有两个标准: DARPA 的通用入侵检测框架中提出的通用入侵规范语言（Common Intrusion Specification Language，CISL）；IETF 的入侵检测工作组（IDWG）中 IAP 使用的另一套方案。两者各有所长，有待进一步研究，以确定一个统一的、能同时实现协作控制信息交换和数据信息交换的通用标准。

入侵检测协作模型应充分利用现有的 Agent 研究成果，并将其应用到入侵检测和攻击防护中；研究 Agent 在安全系统中的角色和与其他安全实体的相互关系；研究 Agent 之间信息交换格式的协作模型；研究各实体之间的分布结构和逻辑从属关系，安全的互操作系统模型等。

（6）建立黑客攻击模型以及主机和网络安全状态模型。对于黑客攻击的识别，现用的方法基本都是在已知攻击的基础上提取其特征，然后将其加入特征库。但是，现有的攻击特征库过于简单，没有扩展性和适应性，造成较高的误报率和漏报率，并缺乏对未知攻击的预警。根据我们的研究和工程经验，建立黑客攻击模型以及主机和网络安全状态模型，可从两方面解决以上问题。

黑客的攻击一般都和大量正常的网络通信混在一起，而对所有海量的审计信息都进行全面检查是十分低效的。我们必须有高效的过程排除噪声，研究现有的黑客攻击方式，归纳出有扩展性和适应性的较通用的几种攻击模型。在实际的检测中，首先应用黑客攻击模型排除绝大多数噪声后记录可疑信息，然后再集中检测具体的攻击形式，这样可大大提高效率，减少误报和漏报；并且只要与该模型匹配的攻击都能被预警，增强了对未知攻击的预警能力。

安全是相对的，所以有必要建立状态模型，以监测主机和网络当前的安全状态。一旦发现异常，很有可能是未知的黑客攻击，可采取应急措施，如进行全面的日志记录，启动一般处于禁止状态的（开销较大的）入侵检测模块，在一段时间内禁止一些危险操作等。对于存放高度机密信息的机构，这种措施尤其有用。安全状态模型应该是通用的，并有可调参数，当系统置于新环境时，可由系统自适应或由安全管理员设定这些参数。

25. 入侵检测技术与法律有什么关系？

答：入侵检测技术（IDS）是通过监视网络或者系统资源，寻找违反安全策略的行为或者攻击迹象，并发出警报。其设计宗旨是预先对入侵活动和攻击性网络流量进行拦截，但

监视网络及网络拦截需要信息网络法的法律支持，使其可以对违反法律的个例予以法律制裁。同时，法律的实施也需要 IDS 的检测。

26. 简述蜜罐技术的特殊用途。

答：蜜罐是一种在互联网上运行的计算机系统，它是专门为吸引并“诱骗”那些试图非法闯入他人计算机系统的人而设计的。

为了吸引攻击者，安全专家通常还在蜜罐系统上故意留下一些安全后门，以吸引攻击者上钩，或者放置一些攻击者希望得到的敏感信息。当然，这些消息都是虚假的信息。蜜罐系统是一个包含漏洞的诱骗系统，它通过模拟一个或多个易受攻击的主机，给攻击者提供一个容易攻击的目标。

最重要的功能是对系统中所有的操作和行为进行监视和记录。另一个用途是拖延攻击者对真正目标的攻击，让攻击者在蜜罐上浪费时间。

这样，最初的攻击目标得到了保护，真正有价值的内容没有受到侵犯。此外，蜜罐也可以为追踪者提供有用的线索，为起诉攻击者搜集有力的证据。

27. 用下载的蜜罐工具构造一个简单的蜜罐系统。

答：所谓的“蜜罐”，就是专门部署一套易被攻击的系统，目标是记录所有攻击者的活动，研究他们的行为，记录他们的 IP 地址，跟踪他们的位置，如果幸运，还能收集到 O-day 漏洞。“蜜罐”系统大多会被设计成一种向攻击者提供任何服务的服务器，从 ssh 到 telnet，开放一些众所周知的可被利用的端口，如 22，23，445，135，139 等。部署蜜罐的服务器需要让攻击者误以为有严重的漏洞，但它实际上是无法有效连接真正有价值的信息的，因此这些漏洞也并不是真正可利用的。设计和部署蜜罐需要谨慎，因为配置不当的蜜罐系统也可能会被攻击者发现，进而产生其他威胁。不过，这种情况超出了本书谈论的范围。在部署蜜罐前，需要了解蜜罐可以被配置为模拟所有可能的系统，从 Apache 服务器到 Windows XP 机器，蜜罐系统上可以运行所有可能的软件和服务。

下面讲述一种简单的部署蜜罐系统的方法，之所以说它简单，是因为你可以用到很多现成的工具。测试环境是 Linux 系统。

Pentbox：个人蜜罐系统。

Pentbox 是一个轻量级的软件，允许打开你的主机端口，监听从外部传入的连接请求（最终是拒绝的）。

步骤如下。

（1）下载 Pentbox：

wget http://downloads.sourceforge.net/project/pentbox18realised/pentbox-1.8.tar.gz。

（2）解压安装包：

tar zxvf pentbox-1.8.tar.gz。

（3）进入 pentbox 目录：

cd pentbox-1.8/。

（4）运行 pentbox：

./pentbox.rb。

28. 收集国内外有关入侵检测、网络诱骗的最新动态。

答：网络诱骗常见的 BOF、Specter、Honeyd 和 ManTrap 等软件，以 Honeyd 为例，其就是一款专用的蜜罐系统构建软件，它不但可以虚拟多种主机，而且对于不同的服务和操作系统的兼容性也较好，其良好实现了伪装真实的目标系统，进而实现攻击者对其进行攻击的目的。此外，蜜罐技术还具有转移攻击者注意力、消耗其攻击资源和意志力的多重作用，从另一个方面实现了保护真实目标系统的目的。所以，使用蜜罐技术作为网络诱骗的技术手段，不但可以减少网络攻击的漏报率和误报率，而且可良好地实现对攻击者新攻击方法和工具的收集，从而实现了诱骗决策的实时调控。为了在大型分布式网络中在部署和维护蜜罐技术时更加方便，必须匹配相应的密场技术，即对各个子网的安全威胁进行集中收集。一般地，其可被视为网络安全工作中的一个重要组成部分，在网络安全管理和研究人员进行网络安全的部署和维护时，由于密场技术的集中性特点，蜜罐技术的维护，数据的更新、分析、管理等工作都会变得较为简单，而且这种密场中集中部署蜜罐的情况也让网络安全风险更易控制。此外，随着网络诱骗系统研发的不断深入，在蜜罐技术系统中，为了更好地保证诱骗系统的高逼真性和可操控性，实现各种攻击信息采集和分析时对多种工具的要求，蜜网概念的提出已势在必行，本质上讲，蜜网即对高交互的蜜罐系统的概括，是诱捕网络体系架构的直接体现，是以高效地收集各种攻击者信息为目的的诱骗技术。当然，虽然蜜网在诱骗系统的响应、分析、检测和恢复等功能上都有显著的提高，但是搭建蜜网需要较高的硬件和管理资本投入，所以其具有一定的局限性。

第 5 章　信息系统安全管理

5.1　第 5 章知识提要

本章习题详细解答了关于信息系统应急响应、数据备份容错和容灾、数字证据获取、安全风险评估和审计、安全测评准则以及开放系统互连安全体系结构等方面的常见问题和实践思路。

5.2　第 5 章习题和答案详解

一、选择题（答案：AABCCD AABBC）

1. 系统备份与普通数据备份的不同在于，它不仅备份系统中的数据，还备份系统中安装的应用程序、数据库系统、用户设置、系统参数等信息，以便迅速________。
   A. 恢复整个系统
   B. 恢复所有数据
   C. 恢复全部程序
   D. 恢复网络设置

答案：A

解答： 系统备份是指备份系统正常运行需要的全部文件以及其他数据，以便在系统出现问题后能够方便地将系统还原到之前备份的状态。

2. 灾难恢复计划或者业务连续性计划关注的是信息资产的_______属性。
   A. 可用性
   B. 真实性
   C. 完整性
   D. 保密性

答案：A

解答： 在美国NIST SP 800-34《信息技术系统应急计划指南》中，将灾难恢复计划（DRP-Disaster Recovery Plan）定义为在紧急事件后在备用场所恢复目标系统、应用或计算机设施的以IT为核心的计划，将业务连续性计划（BCP-Business Continuity Plan）定义为在中断发生或发生后维持组织机构的业务功能。因此，DRP和BCP关注的是信息资产的可用性。

3. 数据备份常用的方式主要有：完全备份、增量备份和________。
A. 逻辑备份
B. 按需备份
C. 差异备份
D. 物理备份

答案：BC

解答：完全备份（full backup）指的是对整个系统或用户指定的所有文件数据进行一次完全的备份。增量备份（incremental backup）只备份上次备份后作过更新的文件。差异备份（differential backup）是每次只备份上次全盘备份之后更新过的数据。按需备份是指在正常的备份之外，有选择地进行的额外备份操作（例如，对于非常关键的数据）。

4. 审计管理是指________。
A. 保证数据接收方收到的信息与发送方发送的信息完全一致
B. 防止因数据被截获而造成的泄密
C. 对用户和程序使用资源的情况进行记录和审查
D. 信息使用者都可有得到相应授权的全部服务

答案：C

解答：安全审计管理的主要活动包括：①选择将被记录和被远程收集的事件。②授予或取消对所选事件进行审计跟踪日志记录的能力。③所选审计记录的远程收集。④准备安全审计报告。

5. 关于安全审计目的的描述，错误的是________。
A. 识别和分析未经授权的动作或攻击
B. 记录用户活动和系统管理
C. 将动作归结到为其负责的实体
D. 实现对安全事件的应急响应

答案：D

解答：信息安全审计主要指按照一定的安全策略，利用记录、系统活动和用户活动等信息检查、审查和检验操作事件的环境及活动，从而发现系统漏洞、入侵行为或改善系统性能的过程。

6. 安全审计跟踪是________。
A. 安全审计系统检测并追踪安全事件的过程
B. 安全审计系统收集易于安全审计的数据的过程
C. 人利用日志信息进行安全事件分析和追溯的过程
D. 对计算机系统中的某种行为的详尽跟踪和观察

答案：A

解答：审计跟踪（audit trail）是指按事件顺序检查、审查、检验其运行环境及相关事件活动

的过程。

7. “保护数据库，防止因未经授权的或不合法的使用造成的数据泄露、更改、破坏。”这是指数据的________保护。

A. 安全性

B. 完整性

C. 并发

D. 恢复

答案：A

解答：保护数据库，防止因未经授权的或不合法的使用造成的数据泄露、更改、破坏。保护数据库，防止因未经授权的或不合法的使用造成的数据泄露、更改、破坏。

8. 信息安全评测标准CC是________标准。

A. 美国

B. 国际

C. 中国

D. 加拿大

答案：B

解答：1993年6月，美国政府同加拿大及欧共体共同起草了单一的通用准则（CC标准）并将其推到国际标准。制定CC标准的目的是建立一个各国都能接受的通用的信息安全产品和系统的安全性评估准则。在美国的TCSEC、欧洲的ITSEC、加拿大的CTCPEC、美国的FC等信息安全准则的基础上，由6个国家（美国、加拿大、英国、法国、德国、荷兰）共同提出了“信息技术安全评价通用准则（The Common Criteria for Information Technology security Evaluation，CC）”，简称CC标准，它综合了已有的信息安全的准则和标准，形成了一个更全面的框架。

9. 我国《信息系统安全等级保护基本要求》中，对不同级别的信息系统应具备的基本安全保护能力进行了要求，共划分为________级。

A. 4

B. 5

C. 6

D. 7

答案：B

解答：《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239—2008）中关于信息系统安全保护等级的定义：信息系统根据其在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高划分为五级，五级定义见GB/T 22240—2008。

10. 在CC中，称为访问控制保护级别的是________。

A. C1

B. B1

C. C2

D. B2

答案：C

解答：C2级系统：在C1级的基础上，通过登录、安全事件和资源隔离增强可调的审慎控制。连接到网上时，用户分别对自己的行为负责。

二、问答题

1. 简述紧急响应的意义。

答：紧急响应的意义主要表现在未雨绸缪和亡羊补牢两个方面。

（1）未雨绸缪，事件发生前做好充分的准备。管理层面进行安全培训，制定安全策略和应急预案，开展风险评估等，技术层面增强系统安全性。

（2）亡羊补牢，事件发生后采取抑制、根除和恢复等措施，尽可能减少损失或尽快恢复正常运行，如收集系统特征，检测病毒和木马等恶意代码，限制或关闭网络服务，系统恢复，反击和跟踪总结等活动。

2. 试述紧急响应服务在实现目的方面受哪些因素制约。

答：紧急响应服务是解决网络系统安全问题的有效服务手段之一，在实施紧急响应时，也受以下方面的制约。

（1）技术复杂性与专业性的制约：当前信息系统、网络、应用涉及各种硬件平台、各类操作系统、种类繁多的应用软件以及形形色色的工作人员，技术的复杂度和处理事件所需的专业程度相当高。

（2）服务人员知识经验的制约：应急响应是由人提供服务，从事应急响应服务的人员应具备丰富的经验，了解频繁发生或可能发生的事件主要类型以及风险。应急响应的成败很大程度上取决于应急服务人员的知识和经验。

（3）事件的突发性：安全事件有可能发生在任何时候、任何场所，对突发情况的反应能力，也是制约应急响应服务的重要因素。

（4）广泛的协调和合作：尽管大多数情况下技术人员是安全事件处理的主要人员，但还需要管理能力、法律知识、人际关系、写作能力、心理学等方面的知识。有效的应急响应不只是简单的技术诊断或凭借技巧解决某些问题，具有不同技能的、具有全面综合能力的团队也是关键因素。

3. 如何制订紧急响应预案？

答：应急响应预案又称应急响应计划，是组织为应对突发或重大信息安全事件而编制的，对包括信息系统运行在内的业务运行进行维持或恢复的策略和规程。

（1）应急响应预案编制准备：进行风险评估、业务影响性分析（BIA），根据风险分析和业务影响分析的结果进行成本效益分析，确定应急响应策略。

（2）应急响应预案编制：一般情况下，应急预案应包括总则、角色及职责、预防和预警机制、应急响应流程、应急响应保障措施和附件六个部分。预案应当描述支持应急操作的技术能力，并适应机构要求。在详细程度和灵活程度之间取得平衡，并根据实际情况对内容进行适当的调整、充实和本地化，应能为信息安全事件中不熟悉计划的人员提供快捷明确的指导。

（3）应急响应预案测试、培训、演练和维护：为了检验预案的有效性，同时使相关人员了解信息安全应急预案的目标和流程，熟悉应急响应的操作规程，应进行应急预案的测试、培训和演练。同时，为了保证应急响应计划的有效性，在以下情况下应对预案进行维护修订：①业务流程编号、信息系统变更、人员变更；②对测试、演练和执行效果进行评估，根据评估情况对预案进行相应修订；③至少每年对预案进行一次评审和修订。

4. 尽可能多地列举一些安全事件。

答：（1）2017 年 2 月，俄罗斯黑帽黑客 Rasputin 利用 SQL 注入漏洞获得了系统的访问权限，黑掉了 60 多所大学和美国政府机构的系统，并从中窃取了大量的敏感信息。遭到 Rasputin 攻击的受害者包括 10 所英国大学、20 多所美国大学以及大量美国政府机构，如邮政管理委员会、联邦医疗资源和服务管理局、美国住房及城市发展部、美国国家海洋和大气管理局等。

（2）2017 年 3 月，维基解密（WikiLeaks）网站公布了大量据称是美国中央情报局（CIA）的内部文件，其中包括了 CIA 内部的组织资料，对计算机、手机等设备进行攻击的方法技术，以及进行网络攻击时使用的代码和真实样本。利用这些技术，不仅可以在计算机、手机平台上的 Windows、iOS、Android 等各类操作系统下发起入侵攻击，还可以操作智能电视等终端设备，甚至可以遥控智能汽车发起暗杀行动。维基解密将这些数据命名为“7 号军火库”（Vault 7），共包含 8761 份文件，即 7818 份网页以及 943 个附件。

（3）2017 年 5 月 12 日，WannaCry 勒索病毒事件全球爆发，以类似于蠕虫病毒的方式传播，攻击主机并加密主机上存储的文件，然后要求以比特币的形式支付赎金。

（4）2017 年 6 月，Petya 勒索病毒的变种开始从乌克兰扩散。与 5 月爆发的 WannaCry 相比，Petya 勒索病毒变种的传播速度更快。它不仅使用了 NSA“永恒之蓝”等黑客武器攻击系统漏洞，还会利用“管理员共享”功能在内网自动渗透。在欧洲国家重灾区，新病毒变种的传播速度达到每 10 分钟感染 5000 余台计算机，多家运营商、石油公司、零售商、机场、ATM 等企业和公共设施已大量沦陷。

（5）2017 年 10 月，一个名为 IoT_reaper 的新型僵尸网络出现。该僵尸网络利用路由器、摄像头等设备的漏洞，将僵尸程序传播到互联网，感染并控制大批在线主机，从而形成具有规模的僵尸网络。目前，很多厂商的公开漏洞都已经被 IoT_reaper 病毒利用，其中包括 Dlink（路由器）、Netgear（路由器）、Linksys（路由器）、Goahead（摄像头）、JAWS（摄像头）、AVTECH（摄像头）、Vacron（NVR）等共 9 个漏洞，感染近 200 万台设备，且每天新增感染量 2300 多次。

（6）安全研究人员在英特尔芯片中发现两个关键漏洞 Meltdown 和 Spectre，利用漏洞攻击者可以从 App 运行内存中窃取数据，如密码管理器、浏览器、电子邮件、照片和文档中的数据，有媒体指出，1995 年之后的每个系统几乎都会受到漏洞的影响，包括计算机和手机，这是非常严重的问题。

5. 简述应急事件处理的基本流程。

答：应急事件处理的基本流程如下。

（1）准备：确定重要资产，分析存在的风险；建立一组针对风险合理的防御/控制措施；建立应急处理策略和在策略指导下的处理程序；建立和训练一个高效率的专业应急响应团队；准备相关的资源。

（2）检测：事件发生后的第一个反应步骤，包括收集信息、初步动作和响应、估计事件范围、初步报告。

（3）抑制：抑制的目的是限制攻击的范围，也就限制了潜在的损失和破坏。

（4）根除：事件被抑制后，接着是找出问题根源和彻底根除安全事件。

（5）恢复：恢复的目标是把所有被攻破的系统和网络设备彻底还原到它们正常的任务状态。

（6）总结：回顾并整合发生事件的相关信息，投入充足的精力与时间对事件进行一次事后的剖析，整理事件与此次响应在技术、过程与其他层面上的信息与收获。

6. 灾难恢复涉及哪些内容？

答：灾难恢复中应当包括如下 10 项内容。

（1）与高层管理人员协商：系统恢复的步骤应当符合组织的安全预案。如果安全预案中没有描述，应当与管理人员协商，以便能从更高角度进行判断，并得到更多部门的支持和配合。

（2）夺回系统控制权：为了夺回对被入侵系统的控制权，需要先将被入侵系统从网络上断开，包括拨号连接。如果在恢复过程中没有断开被侵入系统和网络的连接，入侵者就可能破坏所进行的恢复工作。

（3）复制一份被入侵系统的映像：在进行入侵分析前，最好对被入侵系统进行备份（如使用 UNIX 命令 dd）。这个备份在恢复失败时非常有用。

（4）入侵评估：入侵评估包括入侵风险评估、入侵路径分析、入侵类型确定和入侵涉及范围调查。下面介绍围绕这些工作进行的调查工作。

（5）清除后门：后门是入侵者为下次攻击设下的埋伏，包括修改了的配置文件、系统木马程序，修改了的系统内核等。

（6）查阅 CERT 的安全建议、安全总结和供应商的安全提示：查阅 CERT 以往的安全建议和总结以及供应商的安全提示，一定要安装所有的安全补丁。

（7）记录恢复过程中所有的步骤：毫不夸张地讲，记录恢复过程中采取的每一步措施都是非常重要的。恢复一个被入侵的系统是一件很麻烦的事，要耗费大量的时间，因此经常会使人做出一些草率的决定。记录恢复过程的每一步可以帮助自己避免做出草率的决定，

还可以留作以后参考，也可能给法律调查提供帮助。

（8）系统恢复：各种安全事件预案的执行都是为了使系统在事故后得以迅速恢复。对于服务器和数据库等特别重要的设备，则需要单独制定紧急恢复预案。

（9）改变密码：在弥补了安全漏洞或者解决了配置问题以后，建议改变系统中所有账户的密码。

（10）加固系统和网络的安全：根据 CERT 的配置指南检查系统的安全性，安装安全工具，打开日志，配置防火墙对网络进行防御等。

7. 灾难恢复涉及哪些技术？

答：在灾难恢复中涉及各种可用性、存储备份恢复的技术，如外站仓储、集群技术、复制技术、RAID、全备份/增量备份/差分备份等备份恢复技术、负载均衡技术、NAS/SAN/iSCSI 等存储技术，以及网络、主机、应用领域的技术等。

8. 简述数据容错和数据容灾之间的联系与区别。

答：容错（Fault Tolerant，FT）就是当由于种种原因在系统中出现了数据、文件损坏或丢失时，系统能够自动将这些损坏或丢失的文件和数据恢复到发生事故以前的状态，使系统能够连续正常运行的技术。广泛采用的数据容错技术有双重文件分配表和目录表技术、快速磁盘检修技术、磁盘镜像技术、双工磁盘技术、事务跟踪系统、负载均衡、LOCKSTEP 技术、安全故障（FAILSAFE）软件、服务器容错技术。

真正的数据容灾就是要能在灾难发生时全面、及时地恢复整个系统。在系统遭受灾害时，使系统还能工作或尽快恢复工作的最基础的工作是数据备份。对于一个容灾系统，如果没有备份的数据，任何容灾方案都没有现实意义。从技术上看，衡量容灾系统有两个主要指标——RPO 和 RTO。数据恢复点目标（Recovery Point Object，RPO）主要指的是业务系统所能容忍的数据丢失量，代表了当灾难发生时允许丢失的数据量。恢复时间目标（Recovery Time Object，RTO）主要指的是所能容忍的业务停止服务的最长时间，代表了系统恢复的时间，也就是从灾难发生到业务系统恢复服务功能所需要的最短时间周期。

9. 简述数据备份在数据容错和数据容灾中的作用。

答：数据备份是数据容错和数据容灾的基础。在系统遭受灾害时，使系统还能工作或尽快恢复工作的最基础的工作是数据备份。对于一个容灾系统，如果没有备份的数据，任何容灾方案都没有现实意义。数据容错就是当由于种种原因在系统中出现了数据、文件损坏或丢失时，系统能够自动将这些损坏或丢失的文件和数据恢复到发生事故以前的状态，使系统能够连续正常运行的技术。

10. 简述各种数据备份技术的特点。

答：在备份技术中，有 3 种主要的备份类型。

（1）全备份：对整个系统中的所有文件进行完全备份，包括所有系统和数据。

（2）增量备份：每次备份的数据只是上次备份后更新的数据。

（3）差分备份：每次备份的数据只是上次全盘备份之后更新过的数据。

11. 简述各种数据备份策略的用途。

答：在制定备份策略和选择备份方式时，须综合考虑以下情况。

（1）当备份数据进行大量修改的时候，应先做一次标准备份。而且，标准备份可以作为其他备份的基线。

（2）增量备份最适合用来经常变更数据的备份。

（3）差分备份可以把文件恢复过程简单化。

（4）标准备份与增量或差分备份合用可以做到使用最小的介质保存长期的数据。

12. 收集国内外有关应急响应、数据容错或数字取证的网站信息，简要说明各网站的特点。

答：国内网站：

（1）国家互联网应急中心：http://www.cert.org.cn/。

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是CNCERT或CNCERT/CC）成立于2002年9月，为非政府非营利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。作为国家级应急中心，CNCERT的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行，开展以互联网金融为代表的“互联网+”融合产业的相关安全监测工作。

（2）国家计算机病毒应急处理中心：http://www.cverc.org.cn/。

国家计算机病毒应急处理中心的任务是发现、收集在我国流行的计算机病毒，对计算机病毒进行解剖、分析，向国家CERT中心和公安部提交病毒疫情分析报告，经主管机关授权后发布计算机病毒疫情，建立、维护中国计算机病毒流行列表，为国内用户提供计算机病毒防治的解决方案，指导用户建立和实施计算机病毒防治措施，为有关部门制定我国计算机病毒防治的政策、法规和标准提供技术支持，为遭受计算机病毒攻击破坏的我国计算机用户提供后援服务。

（3）腾讯安全应急响应中心：https://security.tencent.com/。

腾讯安全应急响应中心负责腾讯公司安全漏洞、黑客入侵的发现和处理工作，为安全专家提供在线提交漏洞的平台，提供可以为企业快速构建安全应急响应中心的开放平台xSRC。

（4）360安全应急响应中心：https://security.360.cn/。

360安全应急响应中心成立于2013年，主要针对360集团、控股公司及合作伙伴提供安全应急响应服务，保卫360公司数百款产品的数据安全。

（5）百度安全应急响应中心：http://sec.baidu.com/views/main/index.html#home。

百度安全应急响应中心是百度致力于维护互联网健康生态环境，保障百度产品和业务

线的信息安全，促进安全专家的合作与交流而建立的漏洞收集及应急响应平台，平台收集百度公司各产品线及业务上存在的安全漏洞。

（6）阿里安全响应中心：https://security.alibaba.com/。

阿里安全响应中心隶属于阿里巴巴集团安全部，用于收集阿里巴巴集团各事业部旗下相关产品及业务的安全漏洞和威胁情报，以提升产品及业务的安全性。

（7）京东安全应急中心：http://security.jd.com/。

京东安全应急响应中心是收集京东产品相关的漏洞及威胁情报的窗口。

（8）工业互联网应急响应中心：https://www.ics-cert.org.cn/portal/index.html。

工业互联网应急响应中心提供工业互联网安全的威胁预警、态势感知、检测认证等方面的信息，以及漏洞上报、漏洞查询和漏洞下载功能。

国外网站：

（1）Microsoft Security Response Center

https://technet.microsoft.com/en-us/security/dn440717.aspx。

Microsoft 安全响应中心 (MSRC) 对微软产品的漏洞报告进行调查,并采取了相应的应对措施。

（2）Bitscout

https://securelist.com/bitscout-the-free-remote-digital-forensics-tool-builder/78991/。

Bitscout 是一款可自定义配置的免费的远程数字取证工具。

（3）ProDiscover Forensic

https://www.arcgroupny.com/products/prodiscover-forensic-edition/。

ProDiscover Forensic 可以帮助调查员判断系统是否遭到黑客攻击，可用于在犯罪调查过程中查找犯罪证据。

（4）Volatility Framework

https://github.com/volatilityfoundation/volatility。

Volatility 是一款基于 GNU 协议的开源框架，使用 Python 语言编写而成的内存取证工具集，可以分析内存中的各种数据。Volatility 支持对 32 位或 64 位 Windows、Linux、Mac、Android 操作系统的 RAM（随机存储器）数据进行提取与分析。

（5）Sleuth Kit（+Autopsy）

https://www.sleuthkit.org/。

Sleuth Kit（+Autopsy）是一个开源的电子取证调查工具，它可用于从磁盘映像中恢复丢失的文件，以及为了特殊事件而进行磁盘映像分析。

（6）CAINE（计算机辅助调查环境）

https://www.caine-live.net/。

CAINE（计算机辅助调查环境）是基于 Ubuntu 的 GNU/Linux 自启动运行发行，旨在填补不同取证工具之间的互操作间隙，并提供一致化的图形用户界面，以在电子证据的获取和分析过程中对数字调查进行指导，还为文档和报告的编写提供一个半自动化的过程。

（7）Xplico

https://www.xplico.org/。

Xplico 是一个 IP 流量解码器，用于从互联网流量应用数据中提取数据，是一个 IP/互联网流量的解码器或网络取证分析工具（NFAT）。

（8）X-Ways Forensics

http://www.x-ways.net/forensics/index-c.html。

X-Ways Forensics 是用于计算机取证的综合的取证、分析软件，可在 Windows XP/2003/Vista/2008/7/8/8.1 及 WinPE/FE 操作系统下运行，有 32 位版和 64 位版。

（9）FIRST：https://www.first.org/

FIRST 于 1990 年在美国成立，旨在推动信息分享，在网络安全事件中帮助协调计算机安全事件响应中心（CSIRTs）。在全球范围内，FIRST 的目标是促进事件防范的合作与协调，推动事件快速响应，加强各成员间信息分享。FIRST 还在推广网络安全最佳实践和标准方面发挥着重要作用。

13. 收集国内外有关应急响应、数据容错和数字取证的最新动态。

答：（1）应急响应：当今的网络安全形势严峻，网络威胁发展迅速，应急响应工作面临重大考验。应急响应的发展趋势体现在：在应急处理中开展体系化对抗，从法制、机制、人员、资金、技术等多个层面建立立体对抗体系，用国家力量完成网络应急，完备网络安全应急救援体系，将事后应急向事前和事中应急转变，定期开展国家级、行业级网络安全应急演练。

（2）数据容错：大数据时代来临，信息系统需要存储和处理的数据呈指数级增长，不断增长的海量数据需要被可靠存储，而分布式存储系统庞大的节点规模和数据规模大大提高了发生节点失效的概率，容错技术成为大数据存储中不可忽视的关键技术。

（3）数字取证：随着我国《网络安全法》的实施，数字证据发挥着越来越重要的作用，计算机取证技术成为保证有效执法的关键。目前，计算机取证工具正朝着专业化、自动化、标准化的方向发展。

14. 论述数字证据的特征。

答：数字证据就是在计算机或计算机系统运行过程中产生的、以其记录的内容证明案件事实的电磁记录。与其他证据相比，它有如下特点。

（1）依附性和多样性：电磁证据依附在不同介质上，一是数字证据不会像传统的证据那样可以独立存在；二是不同的介质使同样的信息表现出不同的形态。

（2）可伪性和弱证明性：数字证据的非实物性，使得其窃取、修改，甚至销毁都比较容易。

（3）数据的挥发性：计算机系统中处理的数据有一些是动态的。这些动态数据对于发现犯罪的蛛丝马迹非常有用。但是，它们却有一定的时间效应，即有些数据会因失效或消失而挥发。在收集数字证据时，必须充分考虑数据的挥发性。

15. 上网搜索，提交一份有关数字取证工具的报告。

答：可以参考“22 款受欢迎的计算机取证工具”：

http://www.freebuf.com/sectool/136921.html。

16. 如何保证数字证据的安全？

答：计算机取证中的保护工作主要目的是对目标环境进行保护，避免取证导致证据彻底丢失和数据进一步破坏，保护工作应注意：

（1）保证数据安全性，明确哪些取证操作可能导致证据或数据彻底丢失，避免使用这些类型的操作，如制作磁盘映像，尽量不在原始磁盘上操作。

（2）保证数据完整性，明确哪些取证操作可能破坏证据完整性，取证中不使用可能破坏完整性的操作。

17. 审计与入侵检测技术有什么关系？

答：审计是事后认定违反安全规则行为的分析技术，在检测违反安全规则方面、准确发现系统发生的事件以及对事件发生的事后分析方面发挥巨大作用。入侵检测技术也是通过对计算机网络或计算机系统中的若干收集信息进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。审计侧重于事后分析，两者本质上都是日志分析技术，审计需要对用户行为进行全程记录，入侵检测一般只监控异常或违反规则策略的事件。

18. 简述安全审计的作用。

答：简单地说，安全审计应当具有下面的作用。

（1）记录关键事件。关键事件的界定由安全官员决定。

（2）对潜在的攻击者进行威慑或警告。

（3）为系统安全管理员提供有价值的系统使用日志，帮助系统管理员及时发现入侵行为和系统漏洞，使安全管理人员可以知道如何对系统安全进行加强和改进。

（4）为安全官员提供一组可供分析的管理数据，用于发现何处有违反安全方案的事件，并可以根据实际情形调整安全政策。

19. 简述日志的作用和记录内容。

答：日志（log）是系统指定对象的某些操作和其操作结果按时间有序的集合，是记录信息系统安全状态和问题的原始数据。通常，系统日志是用户可以直接阅读的文本文件。每个日志文件都由日志记录组成，每条日志记录描述了一次单独的系统事件。典型的日志内容有以下几种。

（1）事件的性质：数据的输入和输出、文件的更新（改变或修改）、系统的用途或期望。

（2）全部相关标识：人、设备和程序。

（3）有关事件的信息：日期和时间，成功或失败，涉及因素的授权状态，转换次数，系统响应，项目更新地址，建立、更新或删除信息的内容，使用的程序，兼容结果和参数检测，侵权步骤等。对大量生成的日志，要适当考虑数据的保存期限。

日志文件中的记录可提供以下用途。

（1）监控系统资源；审计用户行为；对可疑行为进行告警。

（2）确定入侵行为的范围；为恢复系统提供帮助；生成调查报告。

（3）为打击计算机犯罪提供证据来源。

20. 审计与入侵检测有什么关联？

答：（1）信息系统安全审计主要指对与安全有关的活动的相关信息进行识别、记录、存储和分析；审计记录的结果用于检查网络上发生了哪些与安全有关的活动，谁（哪个用户）对这个活动负责；主要功能包括安全审计自动响应、安全审计数据生成、安全审计分析、安全审计浏览、安全审计事件选择和安全审计事件存储等。

（2）入侵检测是指检测计算机系统或网络中发生的事件并分析这些事件，以查找可能的事故的过程，这些事故违反或者即将违反计算机安全策略、可接受使用策略或标准安全实践。入侵检测系统（IDS）是自动化入侵检测过程的软件和硬件的组合。

入侵检测一般只监控异常或违法规则策略的事件，并给出报警，而安全审计要保证例行事件和例外事件都能充分记录，以便事后的调查能确定是否有违背安全的事件发生。入侵检测的记录是安全审计的输入之一。

21. 收集国内外有关安全审计的网站信息，简要说明各网站的特点。

答：中华人民共和国审计署：http://www.audit.gov.cn/index.html。

审计署是中华人民共和国国务院 25 个组成部门之一，在国务院总理领导下，主管全国的审计工作。

中国审计网：http://www.iaudit.cn/。

中国审计网的业务涵盖国家审计、内部审计、外部审计、组织治理、风险管理和内部控制等领域。

中国信息系统审计师联盟：http://www.chinacisa.org/。

中国信息系统审计师联盟是一个非营利性的公益组织，旨在为国内信息系统审计相关人员及企业提供一个 IT 治理与风险管理领域互动的沟通平台，分享与完善 IT 风险管理控制体系建设工作经验、IT 审计知识经验，从而促进 CISA 在中国的发展和壮大，以及 IT 审计在中国的实际应用。

国际信息系统审计协会 ISACA：https://www.isaca.org/pages/default.aspx。

国际信息系统审计协会是一个为信息管理、控制、安全和审计专业设定规范的全球性组织。

22. 收集国内外有关安全审计的最新动态。

答：2001 年至今，美国安然事件及由此引发的一系列美国著名大公司在公司治理和财务管理力方面的问题，促使美国陆续出台了多个具有较强影响力的行业法案，如 2002 年美国出台的 Sarbanes-Oxley 法案（塞班斯—奥克斯利法案），其中第 404 条款要求企业在财务报告方面加强内控，企业的 CEO 和 CFO 必须对本企业的内控系统的有效性发表诚信声明。

因此，IT 信息系统同样需要加强控制，以达到 SOX 法案的合规要求；2005 年针对 IT 信息系统的 SOX 合规审计成为全球 CIO 最关注的事。目前，西方发达国家的信息系统审计应用已较普遍，并发展到了较高的水平。信息系统安全审计是信息系统审计全过程的组成部分，主要依据标准包括 COBIT、CC、ITIL 等信息安全管理标准。信息系统安全审计是评判一个信息系统是否真正安全的重要标准之一。通过安全审计收集、分析、评估安全信息、掌握安全状态，制定安全策略，确保整个安全体系的完备性、合理性和适用性，才能将系统调整到“最安全”和“最低风险”的状态。安全审计已成为企业内控、信息系统安全风险控制等不可或缺的关键手段，也是威慑、打击内部计算机犯罪的重要手段。

与国外相比，中国的信息系统安全审计起步较晚，相关信息安全审计技术、信息安全审计规范和信息安全审计制度等都有待进一步完善。1999—2004 年是信息系统安全审计导入期，1999 年财政部颁布了《独立审计准则第 20 号——计算机信息系统环境下的审计》，部分内容借鉴了国外研究成果。这是国内第一次明确提出对计算信息系统审计的要求。2005 年至今，信息系统安全审计进入快速成长期，互联网在国内的迅速普及和应用推动国内信息系统安全审计进入快速发展阶段。国家相关部门、金融行业、能源行业、运营商陆续推出多项针对信息系统风险管理的政策法规，推动国内信息系统安全审计快速发展。目前，随着信息安全建设的深入，安全审计已成为国内信息安全建设的重要技术手段。

23. 风险评估对于信息系统安全有什么意义？

答：从信息安全的角度讲，风险评估是对信息资产面临的威胁、存在的弱点、造成的影响，以及三者综合作用所带来风险的可能性的评估，作为风险管理的基础，风险评估是组织确定信息安全需求的一个重要途径，属于组织信息安全管理体系策划的过程。

信息安全风险评估是信息安全建设的起点和基础。信息安全风险评估工作是科学分析信息和信息系统的保密性、完整性、可用性等方面面临的风险，综合平衡风险大小和管理风险所需付出的代价，在风险的预防、风险的控制、风险的转移、风险的补偿、风险的分散、风险的接受等之间做出合理的选择，只有这样，信息安全建设才能做到从实际出发，才能坚持需求主导、突出重点，才能以最小的代价最大限度地保障安全。

24. 为一个组织的信息系统进行安全风险评估。

答：对一个组织的信息系统进行安全风险评估的流程如图 5-1 所示。具体过程可参考国家标准《GB/T 31509-2015 信息安全技术 信息安全风险评估实施指南》。

25. NAI 公司开发了一个用于安全风险评估的扫描器 CyberCop Scanner，试安装并使用该工具。

答：CyberCop Scanner 能检测出很多漏洞，报告功能也比较强大，还附带有很多实用工具。其中两个很特别的工具是 CASL 和 SMB grinder，CASL 可以以 GUI 方式构建 IP 数据包，而 SMB grinder 具有与 L0phtGrack 类似的口令破解功能。

L0phtGrack 工具：http://www.l0phtcrack.com/

CyberCop Scanner 工具：https://www.exploit-db.com/exploits/39452/

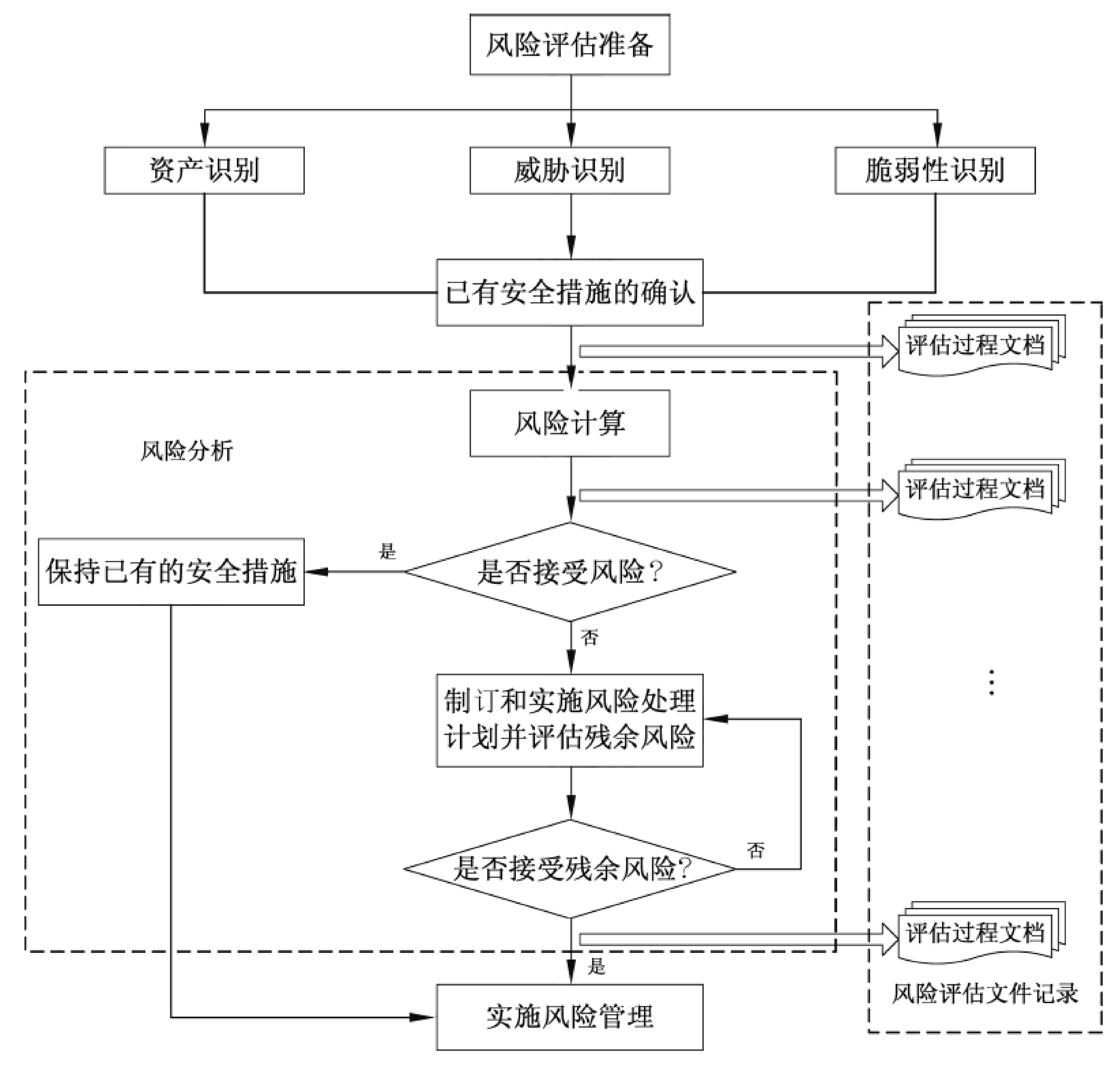


图 5-1　信息安全风险评估实施指南

26. 为学生成绩管理系统设计一个安全策略。这个系统最少要有学生、教师和管理人员访问。

答：假设学生成绩管理系统的基础运行环境（如物理、网络、主机等），已部署和配置适用的安全设备和策略，学校已建立较为完备的信息安全管理体系，在应用和数据层面，设计安全策略时，须考虑以下内容。

（1）学生、教师和系统管理员用户的身份鉴别。对于系统管理员，用户建议采用两种或两种以上组合的鉴别技术实现用户身份鉴别，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。

（2）基于学生、教师和系统管理员用户角色的访问控制。控制用户对文件、数据库表等客体的访问，授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

（3）覆盖每个用户，实现对学生成绩管理系统重要安全事件的审计。

（4）保证通信过程的完整性和保密性。

（5）关键数据的完整性、保密性保护，以及备份和恢复。

27. 在一个具有读、写、准许和取消 4 种访问操作的系统中，准许操作可以授予其他主体读和写的访问权限，并且还可以授予其他主体发布对你拥有的资源的访问权限。如果要

使用准许和取消操作控制对你拥有的一个客体的所有访问，应当采用什么样的数据结构和算法实现准许和取消操作。

答：根据题意，需要实现的功能是自主访问控制，可以采用访问控制矩阵（ACM）实现准许和取消操作。访问控制矩阵是一个包含有主体和客体的表，它规定每一个主体对每一个客体所能执行的操作。

28. 给出一个中等规模的局域网（包含一些子网，但不跨多个地域），为其设计一个安全解决方案。

答：在设计安全解决方案前，应明确该局域网所承载的业务系统、网络结构、网络应用，分析网络系统面临的信息安全风险，包括物理层面、网络层面、主机层面、应用和数据层面的安全分析以及管理风险，基于风险分析结果明确局域网安全需求，进而选择能够满足安全需求的安全机制和安全措施。一般情况下，对于中等规模的局域网，其网络层面的安全解决方案应考虑以下内容。

（1）网络结构安全：包括主要设备的业务处理能力、带宽、路由控制、子网划分、网段间隔离等。

（2）访问控制：明确网络边界，在边界部署访问控制设备，启用访问控制功能，对应用层协议进行过滤与控制，对重要子网或网段采取技术手段防止地址欺骗，按照用户与系统之间的允许访问规则实现访问控制等。

（3）安全审计：对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录并分析，保护审计记录。

（4）边界完整性：防止非法接入网络或内部用户非法外联。

（5）入侵防范：在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等。

（6）恶意代码防范：在网络边界处对恶意代码进行检测和清除。

（7）网络设备防护：网络设备用户的身份鉴别、网络设备管理员登录限制等。

29. 分析一个具体系统的安全需求，并给出相应的安全策略。

答：对于一个具体系统，首先对系统进行安全风险评估，确定安全需求，并制定相应的安全策略。

（1）收集系统所有相关信息，如网络拓扑、系统结构、业务流程、系统的操作运行情况、物理环境、未来规划等，对系统现有的安全措施也要进行了解确认。

（2）选择一个适合的安全基线，根据系统安全等级和安全目标，结合系统实际情况对基线要求进行裁剪或增强，作为系统安全需求的输入。

（3）确定系统的关键资产，分析威胁、脆弱性，评估系统的安全风险。

（4）按照系统可接受的风险尺度确定存在的各个风险的处理策略，如转移、规避、降低或接受。

（5）需要转移和规避的风险由系统规划作总体考虑，需要降低的风险作为安全需求的输入。

（6）根据风险评估确定的安全需求，选择能够满足安全需求的安全机制和安全措施。

（7）完成安全机制和安全措施实施后，应评估确认是否满足了安全需求，将系统风险控制在可接受范围。

30. 如何理解 OSI 安全体系的安全机制和安全服务之间的对应关系？

答：OSI 安全体系结构给出了 8 种基本（特定的）安全机制，包括加密、数字签名、访问控制、数据完整性、认证、业务流填充、路由控制、公正机制，使用这 8 种安全机制，再加上几种普遍性的安全机制，将它们设置在适当的（N）层上，用以提供 OSI 安全体系结构 5 类安全服务，即认证（鉴别）服务、访问控制服务、数据保密性服务、数据完整性服务、抗否认性服务。安全机制和安全服务之间的对应关系如图 5-2 所示。

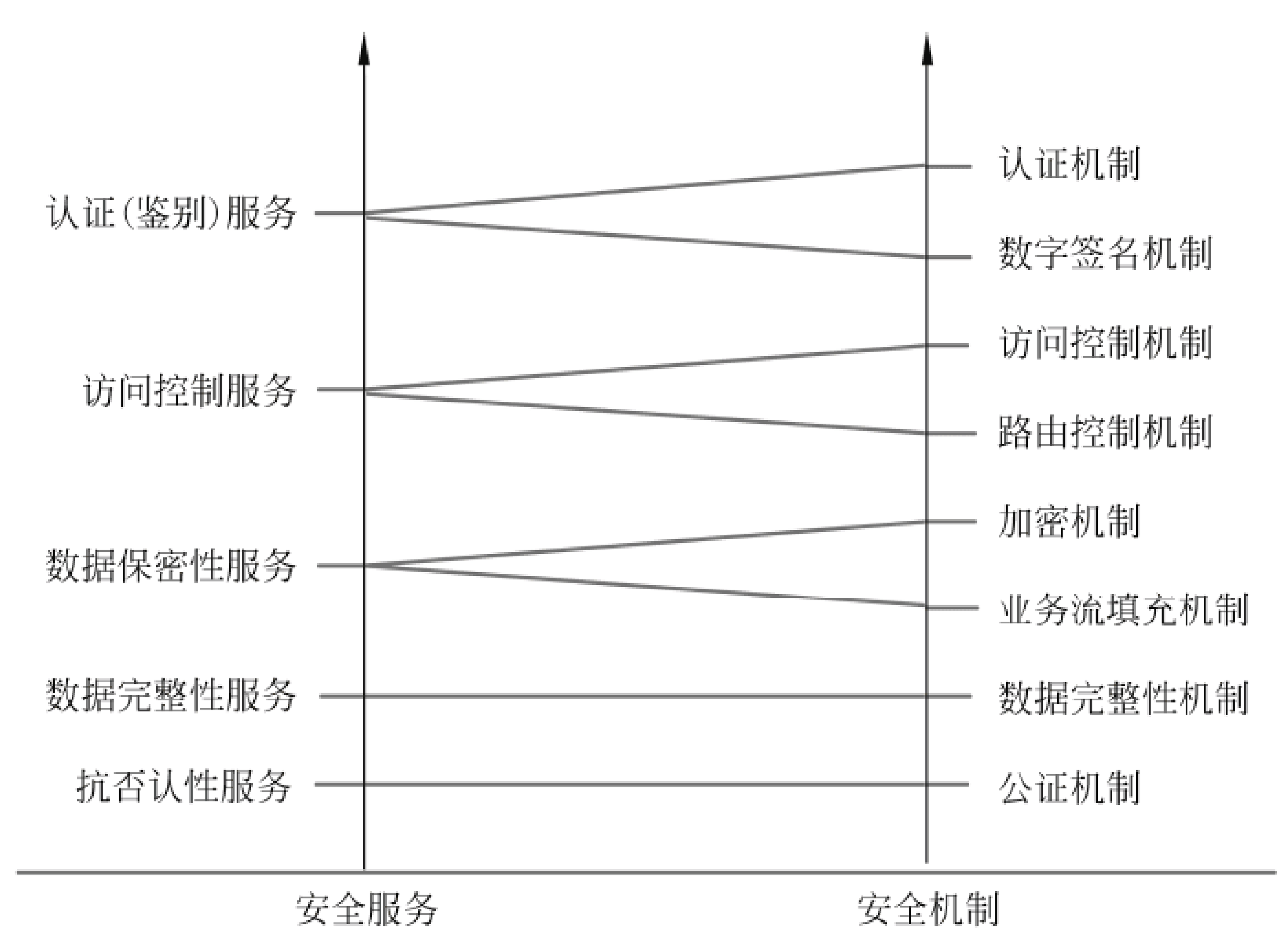


图 5-2　安全机制和安全服务之间的对应关系

31. 什么是可信计算基？

答：在信息安全等级标准中，一个非常重要的概念是可信计算基（Trusted Computer Base，TCB）。TCB 是计算机系统赖以实施安全性的一切设施，包括硬件、固件、软件和负责安全策略的组合。它们根据安全策略处理主体（系统管理员、安全管理员、用户和进程）对客体（如进程、文件、记录和设备等）的访问，通常包括下列部分。

（1）操作系统的安全内核。

（2）具有特权的程序和命令。

（3）处理敏感信息的程序，如系统管理命令等。

（4）与 TCB 实施安全策略有关的文件。

（5）其他有关的固件、硬件和设备。

（6）负责系统管理的人员。

（7）保障固件和硬件正确的程序和诊断软件。

（8）具有抗篡改的性能和易于分析与测试的结构。

32. 详细说明安全标记保护级的可信计算基的功能。

答： 安全标记保护级的可信计算基具有系统审计保护级的所有功能。此外，还需以访问对象的安全级别限制访问者的访问权限，实现对访问对象的强制访问。具体保护能力如下。

（1）自主访问控制：同系统审计保护级。

（2）强制访问控制：可信计算基对所有主体及其控制的客体（如进程、文件、段和设备）实施强制访问控制。通过敏感标记为这些主体及客体指定安全等级。安全等级用二维组表示：第一维是等级分类（如秘密、机密和绝密等），第二维是范畴（如适用范畴）。它们是实施强制访问控制的依据。可信计算基支持两种或两种以上成分组成的安全级。可信计算基控制的所有主体对客体的访问应满足以下要求。

① 仅当主体安全级中的等级分类高于或等于客体安全级中的等级分类，且主体安全级中的非等级类别包含了客体安全级中的全部非等级类别，主体才能读客体。

② 仅当主体安全级中的等级分类低于或等于客体安全级中的等级分类，且主体安全级中的非等级类别包含了客体安全级中的全部非等级类别，主体才能写一个客体。

可信计算基使用身份和鉴别数据鉴别用户的身份，并保证用户创建的可信计算基外部主体的安全级和授权受该用户的安全级和授权的控制。

（3）敏感标记：是实施强制访问的基础。可信计算基应明确规定需要标记的客体（如进程、文件、段和设备），明确定义标记的粒度（如文件级、字段级等），并必须使其主要数据结构具有相关的敏感标记。为了输入未加安全标记的数据，可信计算基向授权用户要求并接受这些数据的安全级别，且可由计算机信息系统可信计算基审计。

（4）身份鉴别：可信计算基初始执行时，首先要求用户标识自己的身份，而且，可信计算基维护用户身份识别数据并确定用户的访问权及授权数据。其他同系统审计保护级。

（5）客体重用：同系统审计保护级。

（6）审计：在系统审计保护级的基础上，要求可信计算基具有审计更改可读输出记号的能力。

（7）数据完整性：可信计算基通过自主和强制完整性策略，阻止非授权用户修改或破坏敏感信息。在网络环境中，使用完整性敏感标记确保信息在传送中未受损。

33. 结构化保护级的主要特征有哪些？

答： 与安全标记保护级相比，结构化保护级的主要特征如下。

（1）可信计算基基于一个明确定义的形式化安全保护策略。

（2）将第三级实施的（自主或强制）访问控制扩展到所有主体和客体，即在自主访问控制方面，可信计算基应维护由外部主体能够直接或间接访问的所有资源（如主体、存储客体和输入输出资源）实施强制访问控制，为这些主体及客体指定敏感标记，这些标记是等级分类和非等级类别的组合，它们是实施强制访问控制的依据。

（3）审计。

① 同系统安全标记保护级。

② 计算机信息系统可信计算基能够审计利用隐蔽存储信道时可能被使用的事件。

（4）数据完整性。计算机信息系统可信计算基通过自主和强制完整性策略，阻止非授权用户修改或破坏敏感信息。在网络环境中，使用完整性敏感标记确保信息在传送中未受损。

（5）隐蔽信道分析。系统开发者应彻底搜索隐蔽存储信道，并根据实际测量或工程估算确定每一个被标识信道的最大带宽。

（6）可信路径。对用户的初始登录和鉴别，计算机信息系统可信计算基在它与用户之间提供可信通信路径，该路径上的通信只能由该用户初始化。

34. 收集有关信息安全的定义、标准等方面的最新概念和进展。可以从下面的网站开始。

http://www.radium.ncsc.mil/tpep/process/fag.html

http://www.itsec.gov.uk

http://www.cse-cst.gc.ca/pub/criteria/CTCPE

答：国内信息安全定义、标准方面的最新概念和进展可以从全国信息安全标准化技术委员会 TC260 等的官方网站获取：https://www.tc260.org.cn/。

国际信息安全定义、标准方面的最新概念和进展可以从国际标准化组织 ISO/IEC JTC1 SC27、美国 NIST、欧盟 ENISA 等的官方网站获取。

https://www.iso.org/committee/45306/x/catalogue/

https://www.nist.gov/

https://www.enisa.europa.eu/

35. 收集资料，分别给出下列操作系统的安全等级，并说明理由。

（1）DOS。

（2）Windows。

（3）UNIX。

（4）Linux。

答：TCSEC 是计算机系统安全评价的第一个正式标准，于 1970 年由美国国防科学技术委员会提出，于 1985 年 12 月由美国国防部公布。TCSEC 把计算机系统的安全分为 A、B、C、D 4 等 7 级。D 等为最低级别，C 等为自主保护级别，B 等为强制保护级别，A 等为验证保护级别。

DoS 系统被定义为 D1 级，因其未加任何实际的安全措施，所以只为文件和用户提供安全保护。属于这个基本的操作系统还有 Windows 95 和 Windows 98。

Windows NT、Windows 2000、Windows 2003、UNIX、Linux 系统均能达到 C2 级别。C1 级系统要求硬件有一定的安全机制（如硬件带锁装置和需要钥匙才能使用计算机等），用户在使用前必须登录到系统。C1 级系统还要求具有完全访问控制的能力，应当允许系统管理员为一些程序或数据设立访问许可权限。C1 级防护的不足之处在于用户直接访问操作系统的根。C1 级不能控制进入系统的用户的访问级别，所以用户可以将系统的数据任意移走。C2 级在 C1 级的某些不足之处加强了几个特性，C2 级引进了受控访问环境（用户权限

级别）的增强特性。这一特性不仅以用户权限为基础，还进一步限制了用户执行某些系统指令。授权分级使系统管理员能够分用户分组，授予他们访问某些程序的权限或访问分级目录。另一方面，用户权限以个人为单位授权用户对某一程序所在目录的访问。如果其他程序和数据也在同一目录下，那么用户也将自动得到访问这些信息的权限。C2 级系统还采用了系统审计。审计特性跟踪所有的“安全事件”，如登录（成功的和失败的），以及系统管理员的工作，如改变用户访问和口令。

36. 写出以下与信息安全相关的英文缩写的全称。

FTP，HTTP，NFS，DNS，UDP，TCP，IP；

ICMP，SMTP，SNMP，POP，IMAP；

S/MIME，TFTP，TELNET；

Rlogin，RPC，NFS，NIS；

DCOM，ISN，SRC；

SYN，ACK，RST，FIN。

答：

FTP：File Transfer Protocol　文本传输协议

HTTP：Hypertext Transfer Protocol　超文本传输协议

NFS：Network File System　网络文件系统

DNS：Domain Naming Service　域名服务

UDP：User Datagram Protocol　用户数据协议

TCP：Transmission（Transport） Control Protocol　传输控制协议

IP：Internet Protocol　网络协议

ICMP：Internet Control Message Protocol　网络控制信息协议

SMTP：Simple Mail Transport Protocol　简单邮件传输协议

SNMP：Simple Network Management Protocol　简单网络管理协议

POP：Post Office Protocol　邮局协议

IMAP：Internet Message Access Protocol　网络信息接入协议

S/MIME：Secure/Multipurpose Internet Mail Extension　安全版本/多用途网际邮件扩充协议

TFTP：Trivial File Transfer Protocol　小文件传输协议

TELNET：Tele Network　远程网络

Rlogin：Remote Login　远程登录

RPC：Remote Procedure Call　远程过程调用

NFS：Network File System　网络文件系统

NIS：Network Information Service　网络信息服务

DCOM：Distributed Component Object Model　分布式组件对象模型

ISN：Initial Sequence Number　初始序列号

SRC：Source　源

SYN：Synchronization Sequence Number　同步序列号

ACK：Acknowledge Character　确认字符

RST：Reset　复位

FIN：Finish　结束

附 2017 年信息安全专业综合考题及答案

附 1　综合考题一及答案

一、选择题（每小题 2 分，共 40 分）

1. 信息系统安全在不同的环境和应用中会得到不同的解释。解释________是不正确的。
   A. 数字信息处理系统安全，即保证数字信息处理过程中无错误
   B. 网络上系统信息的安全，包括用户口令鉴别、用户存取权限控制、数据存取权限、方式控制、安全审计、安全问题跟踪、计算机病毒防治和数据加密等
   C. 网络上信息传播的安全，即信息传播后的安全，包括信息过滤等。它侧重于保护信息的保密性、真实性和完整性。避免攻击者利用系统的安全漏洞进行窃听、冒充和诈骗等有损于合法用户的行为
   D. 网络系统的硬件、软件及其系统中的数据受到保护，不因偶然因素而遭到破坏、更改或泄露，系统连续、可靠、正常地运行，服务不中断

2. 信息系统安全应具有4个方面的特征，________不是信息系统安全的特征。
   A. 保密性，指信息不泄露给非授权用户、实体或过程，或供其利用的特性
   B. 完整性，指数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性
   C. 可执行性，指可被授权实体允许执行
   D. 可控性，指对信息的传播及内容具有控制能力

3. 信息系统安全来自许多威胁因素，下面的答案中________不是信息系统安全的威胁因素。
   A. 非人为的、自然力造成的数据丢失、设备失效、线路阻断
   B. 人为的，但属于操作人员无意的失误造成的数据丢失
   C. 来自外部和内部人员的恶意攻击和入侵
   D. 个人学习系统

4. TCP FIN扫描属于________技术。
   A. 主机扫描
   B. 端口扫描
   C. 漏洞扫描
   D. 远程操作系统识别

5. ProtectX属于________。
A. 端口扫描监测工具
B. 木马检测工具
C. 缓冲区溢出监测工具
D. 网络嗅探软件

6. 以下关于交换式局域网中存在网络嗅探的隐患原因，不正确的是________。
A. 交换设备信息过载
B. ARP欺骗
C. 跨站脚本攻击
D. TCP会话劫持

7. 通常情况下，客户主机需要访问www.dhs.com时，首先要知道www.dhs.com的IP地址。而客户主机获得www.dhs.com IP地址的唯一方法是向其所在网络的DNS服务器进行查询。一次DNS域名解析过程随即展开。________是DNS欺骗攻击者可能做篡改的。
A. 客户主机软件（如Web浏览器）需要对www.dhs.com进行解析。它首先会向本地DNS服务器（nipc.com域）发送域名解析请求，要求告知www.dhs.com的IP地址
B. 本地DNS服务器的数据库中没有www.dhs.com的记录，缓存中也没有相应记录，所以它会依据DNS协议机器配置向网络中的其他DNS服务器提交请求。这个查询请求将逐层递交，直到dhs.com域的DNS服务器收到请求（这里省略了寻找dhs.com域DNS服务器的迭代过程，假定本地DNS服务器最终找到了需要的信息）
C. dhs.com域DNS服务器将向nipc.com域DNS服务器返回IP查询结果（假定查询结果为1.2.3.4）
D. nipc.com域的本地DNS服务器最终将查询结果返回给客户主机浏览器，并将这一结果存储到其DNS缓存中

8. 防范会话劫持攻击有很多方法，________方法是不恰当的。
A. 进行加密
B. 使用安全协议
C. 限制保护措施
D. 身份认证

9. 以下关于强口令的特征中，________是不正确的。
A. 每45天换一次
B. 可以包含词典中的单词
C. 至少包含10个字符
D. 必须包含一个字母、一个数字、一个特殊的符号

10. 以下关于蜜罐技术的说法，________是不正确的。
   A. 蜜罐系统主动吸引攻击者，记录并分析攻击者的攻击行为
   B. 蜜罐系统拖延攻击者对真正目标的攻击
   C. 只要攻击者入侵蜜罐的某项服务，系统就会记录下它们的行为并观察它们接下来的所有动作
   D. 蜜罐系统是一种安全解决方案，会“修补”发现的所有错误

11. ________不属于动态网页技术。
   A. MATLAB
   B. ASP
   C. CGI
   D. PHP

12. 下面关于RSA算法，正确的是________。
   A. RSA属于非对称密码算法
   B. RSA属于对称密码算法
   C. RSA仅可以用于数字加密，不可以用于数字签名
   D. RSA不会被黑客利用

13. DES的最大缺陷在于________。
   A. 除S盒外，都使用了标准的算术和逻辑运算
   B. 密钥长度较短，经不住穷举攻击
   C. DES的“雪崩效应”，即明文或密钥的微小改变将对密文产生很大影响
   D. S盒可能存在陷门

14. ________不属于用户身份认证的范畴。
   A. 基于被验证者所知道的（知识证明）
   B. 基于被验证者所拥有的（持有证明）
   C. 基于被验证者的生物特征（属性证明）
   D. 基于被验证者的家属指纹

15. 第三方日志工具的作用不包括________。
   A. 很少有入侵者能掌握众多的第三方日志软件的入侵和攻击知识
   B. 好的第三方日志软件能够单独获得日志信息，不需要操作系统日志文件作为开始的索引。因此，可以利用这些信息与操作系统的日志信息进行对比，当发现不一致时，管理员立即可以知道有人入侵了系统
   C. 修改banner
   D. 当系统日志工具出现问题时，第三方日志产品可起到类似备份的作用

16. ________不属于木马技术。

A. 自我复制技术

B. 自动加载运行技术

C. 远程监控技术

D. 动态嵌入技术

17. 下面关于宏病毒的说法，正确的是________。

A. 宏病毒只感染Word和Excel文件

B. 正是有了足够强大的宏语言的支持，宏病毒才得以迅速发展

C. 1985年8月出现了第一个宏病毒Word Macro/Concept

D. 相对而言，宏病毒难以编写

18. 关于蠕虫和病毒之间的区别，说法不正确的是________。

A. 蠕虫与病毒最大的区别在于它自身的主动性和独立性

B. 病毒需要插入到宿主文件中，而蠕虫是利用计算机系统的漏洞进行传播

C. 病毒的触发传染来自程序自身，而蠕虫的触发传染来自计算机使用者

D. 病毒的影响重点是文件系统，蠕虫的影响重点是网络和系统性能

19. 代理服务器型防火墙实现的功能不包括________。

A. 用户认证

B. 将所有的内部IP地址都映射到防火墙使用的另一个安全IP地址上

C. 审计跟踪

D. 数据加密

20. 虚拟专用网采用的安全技术不包括________。

A. 安全隧道技术

B. 访问控制技术

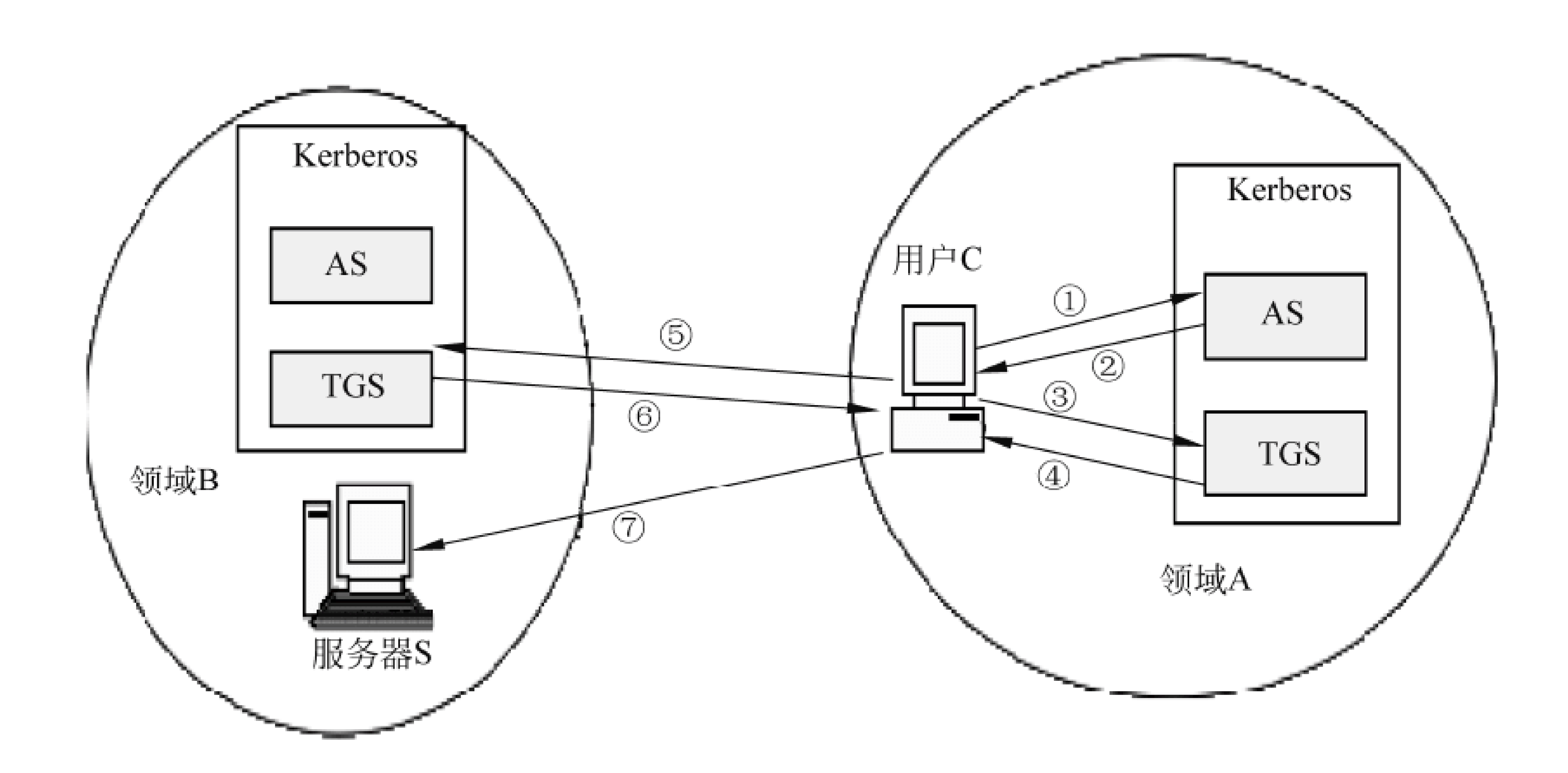
C. 入侵检测技术

D. 加密技术

二、填空题（每小题 2 分，共 20 分）

1. 计算机病毒的5个特征是：主动传染性、破坏性、________、寄生性（隐蔽性）和________。计算机病毒是________，它能够侵入计算机系统，并且能够通过修改其他程序，把自己或者自己的变种复制插入其他程序中；这些程序又可传染别的程序，实现繁殖传播。

2. Kerberos异域认证系统的工作过程如下。



① C→AS：E_{KC} [________ || ID_T ||TS_1]。

② AS→C：E_{KC}[K_{CT} ||ID_T || TS_2 ||________|| $Ticket_{TGS}$]。

③ C→TGS：E_{KCT}[ID_{TB} || $Ticket_{TGS}$ || $Authenticator_C$]（ID_{TB} 为 B 域 TGS_B 标识）。

④ TGS→C：E_{KCT}[K_{CTB}||ID_{TB}||TS_4|| $Ticket_{TB}$]（K_{CTB} 为 C 与 TGS_B 会话密钥）。

$Ticket_{TB}$= E_{KTB}[K_{CTB}||ID_C||AD_C ||ID_{TB}||TS_4||$Lifetime_4$]

⑤ C→TGS_B：E_{KCTB}[ID_{TB}||$Ticket_{TB}$||$Authenticator_C$]。

⑥ TGS_B→C：E_{KCTB}[K_{CS} || ID_{TB} ||TS_6 || $Ticket_{TB}$]。

⑦ C→S：E_{KCS}[$Ticket_{TB}$||________]。

其中，K_C为C的用户主密钥，由C上的用户口令导出；可与AS共享，记为K_{CA}。

K_S为S服务器主密钥，可与TGS共享，也记为K_{ST}。

K_T为TGS主密钥，可与AS共享，记为K_{AT}。

K_{CT}为C与TGS会话密钥。

K_{TS}为TGS与S会话密钥。

K_{CS}为C与S会话密钥。

3. 网卡有以下四种工作模式：________，________，________ 和 ________。

三、计算题（共 20 分）

1. 设通信双方使用 RSA 加密体制，接收方的公开密钥是(e, n)=(3,77)，求明文 M=30 对应的密文。（5 分）

2. 假定允许使用 26 个大写字母，26 个小写字母（严格区分大小写）和 10 个数字构造口令，口令长度为 9 个字符，若采用暴力攻击，则在下列情况下各需要多少时间（精确到小数点后 4 位即可）？（1）检查一个口令需要 1/10s 时间。（2）检查一个口令需要 1ns 时间。（7 分）

3. 设明文 M= good luck，密钥 K= test，则采用维吉尼亚密码的加密字母是什么？十六进制 ASCII 编码输出是什么？（8 分）

维吉尼亚编码规则为：给出密钥 K=$k[1]k[2]\cdots k[n]$，若明文为 M=$m[1]m[2]\cdots m[n]$，则对应的密文为 C=$C[1]C[2]\cdots C[n]$，其中，$C[i]$=$(m[i]+k[i])$ mod 26。维吉尼亚方阵如下所示。

明文	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
…																										
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
…																										
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
…																										
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

四、简答题（20 分）

1. 可以采用哪些技术防御扫描攻击？（5 分）

2. 请详细说明下列程序中是否存在缓冲区溢出？（5 分）

```
# include <stdio.h>
main()
{
int num= 0x61616161;
printf ("Before : num = %#x \n", num);
printf ("%.20d %n \n", num, &num);
printf ("After : num = %#x \n", num);
}
```

3. 跨站脚本攻击是如何实现的？应如何防御？（5 分）

4. 请说明分布式拒绝服务攻击的原理。（5 分）

综合考题一答案

一、1. A　2. C　3. D　4. B　5. A　6. C　7. C　8. D　9. B　10. D
11. A　12. A　13. B　14. D　15. C　16. A　17. C　18. C　19. B　20. C

二、

1. 非授权执行性，可触发性，一段程序代码

2. ID_C,$Lifetime_2$,$Authenticator_C$

3. 广播模式、组播模式、直接模式、混杂模式

三、

1. 接收方的公开密钥是(e, n)=(3,77)

明文 M=30 经过加密后为 50，即对应的密文为 C=50。

2. 可能产生口令长度为 9 的口令总数量为 62 的 9 次方=1.3537e16 个，因此，如果检查一个口令的时间为 1/10s 时，暴力攻击穷举搜索最长的攻击时间为 1.3537e15s，相当于 2.2562e14min，也就是 3.7603e12h，等于 1.5668e11 天，相当于 4.2926e8 年的时间。

如果检查一个口令需要 1ns 时间，也就是前面单位时间的 10e(−8)，则穷举搜索完毕需要 4.2926 年。

3. 加密字母是 ZSGW EYUD，十六进制 ASCII 编码输出是 5A 53 47 57 45 59 55 44。

四、

1. 采用端口扫描监测工具，采用个人防火墙，针对 Web 服务的日志审计，修改 Banner。

2. 存在。参数&num 要比参数 num 先压入栈中，这是因为带有可变参数的函数使用 C 函数调用约定，参数从右向左依次压栈，栈中的内容在被调用函数返回后由程序自动删除。整个程序的输出结果为

Before : num = 0x61616161

0000000001633771873

After : num = 0x14

我们看到，变量 num 的值已经变成了 0x14(20)。也就是说，因为程序中将变量 num 的地址压入堆栈作为 printf()的第三个参数，而使用打印格式%n 会将打印总长度保存到对应参数（&num）的地址中，从而改变了 num 的值。

3. 跨站脚本（Cross-Site Scripting，XSS）攻击指的是恶意攻击者往 Web 页面里插入恶意的代码或数据，当用户浏览该页面时，嵌入其中的脚本会被解释执行。攻击者因此可以绕过文档对象模型（DOM）的安全限制措施，进行恶意操作，如 Cookies 窃取、更改 Web 应用账户设置、传播 Web 邮件蠕虫等。存在 XSS 漏洞的 Web 组件包括 CGI 脚本、搜索引擎、交互式公告板等。

跨站脚本漏洞主要是由于 Web 服务器没有对用户的输入进行有效性验证或验证强度不够，而又轻易将它们返回给客户端造成的。Web 服务器允许用户在表格或编辑框中输入不相关的字符，Web 服务器存储并允许把用户的输入显示在返回给终端用户的页面上，而这个回显并没有去除非法字符或者重新进行编码。

针对 XSS 攻击，对普通浏览网页用户及 Web 应用开发者给出的安全防御建议如下。

对于普通浏览网页用户，在网站、电子邮件或者即时通信软件中单击链接时需要格外小心：留心可疑的过长链接，尤其是它们看上去包含了 HTML 代码。还可以安装一些浏览器插件，如 Firefox 的 NoScript 或者 Netcraft 工具条，并且尽量避免访问有问题的站点。

对于 Web 应用开发者，首先应该把精力放到对所有用户提交内容进行可靠的输入验证上。这些提交内容包括 URL、查询关键字、post 数据等。只接受在你规定长度范围内、采用适当格式的字符，阻塞、过滤或者忽略其他任何东西。保护所有敏感的功能，以防被机器人自动执行或者被第三方网站所执行。可采用的技术有 session 标记（session tokens）、验证码。如果你的 Web 应用必须支持用户提交 HTML，确认你接收的 HTML 内容被妥善地格式化，仅包含最小化的、安全的 tag（绝对没有 JavaScript），去掉任何对远程内容的引用（尤其是 CSS 样式表和 JavaScript）。

4. DDoS 攻击通常借助客户/服务器技术。在进行 DDoS 攻击前，攻击者必须先用其他手段获取大量傀儡主机的系统控制权，用于安装进行拒绝服务攻击的软件。这些傀儡主机最好具有良好的性能和充足的资源，如强的计算能力和大的带宽等。

用于 DDoS 攻击的软件一般分为守护端（安装守护端的主机称为代理）与服务端（安装服务端的主机称为主控）。这些程序可以协调，使分散在互联网各处的机器共同完成对一台主机的攻击操作。

当需要攻击时，攻击者连接到安装了服务端软件的主控，向服务端软件发出攻击指令，主控在接收到攻击指令后，控制多个代理同时向目标主机发动猛烈攻击。通常，主控与代理之间并不是一一对应关系，而是多对多的关系。也就是说，一个安装了代理的服务器可以被多个主控所控制，一个主控也同时控制多个代理。图 1 是三层结构的 DDoS 攻击示意图。采用这种三层结构可以确保入侵者的安全。攻击者发出指令后，就可以断开连接，由主控负责指挥代理展开攻击。因此，攻击者连接网络和发送指令的时间很短，隐蔽性极强。

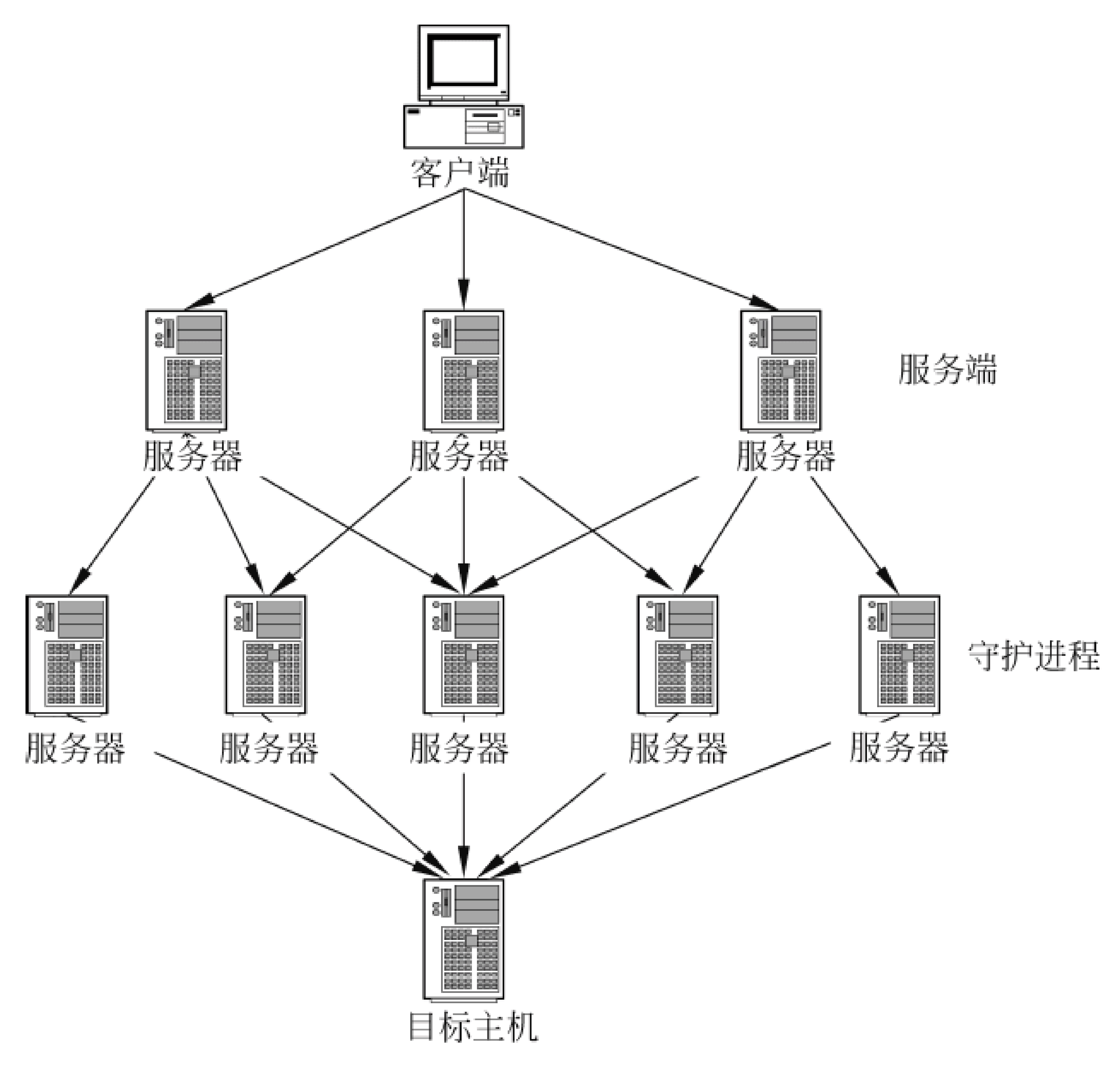


图 1　三层结构的 DDoS 攻击示意图

目前流行的分布式拒绝服务攻击软件一般没有专用的客户端软件，而是使用 Telnet 方式进行连接和控制命令传送。

由于 DDoS 攻击同时使用多台主机进行攻击，攻击者来自范围广泛的 IP 地址，防御变得困难，而且来自每台主机的数据包数量都不大，因此很有可能从入侵检测系统（Intrusion Detection System，IDS）的眼皮下溜掉，探测和阻止也就变得更加困难。目前而言，攻击者基本上都抛弃了原始的使用简单几台主机进行 DoS 攻击的方式，转而使用这种规模更大、威力更强、成功率更高、效果更明显、追踪更困难的 DDoS 攻击。

附 2　综合考题二及答案

一、选择题（每小题 2 分，共 20 分）

1. FTP的英文全称是________。
   A. File Transfer Protocol
   B. Finished Text Program
   C. Fly Task Pen
   D. Full Time Program

2. 电子信息化体现在生活的方方面面，________不属于电子信息化的体现。
   A. 支付宝
   B. 电子银行
   C. 网络图书馆
   D. 和客户咖啡馆见面

3. 关于0day漏洞，定义正确的是________。
   A. 是一种对黑客来说很易攻击，对管理者来说不费吹灰之力就可以修补的漏洞
   B. 顾名思义，还没有出现的漏洞叫0day漏洞
   C. 是指在操作系统安全补丁发布前被了解和掌握的漏洞信息
   D. 是一种程序上的不完善

4. Don’t Fragment（DF）位探测属于________。
   A. 主机扫描
   B. Ping扫描
   C. 漏洞扫描
   D. 远程主机操作系统指纹识别

5. SATAN属于________。
   A. 网络嗅探软件

B. 木马检测工具
C. 缓冲区溢出监测工具
D. 端口扫描工具

6. 以下关于共享式网络下防监听方法不正确的是________。
A. 网络响应时间测试
B. ARP检测
C. 跨站脚本攻击
D. 主机响应时间测试

7. 数字签名要预先使用单向Hash函数进行处理的原因是________。
A. 多一道加密工序使密文更难破译
B. 提高密文的计算速度
C. 缩小签名密文的长度，加快数字签名和验证签名的运算速度
D. 保证密文能正确还原成明文

8. ________不属于木马技术。
A. 自我复制技术
B. 自动加载运行技术
C. 远程监控技术
D. 动态嵌入技术

9. 口令破解的常用方法中，________属于社会工程学。
A. 穷举法
B. 通过嗅探和木马等手段获取口令
C. 自动口令破解器
D. 假扮技术支持获取远程计算机的访问权

10. 以下关于蜜罐技术的说法，不正确的是________。
A. 蜜罐系统主动吸引攻击者，记录并分析攻击者的攻击行为
B. 蜜罐系统是一种安全解决方案，会“修补”发现的所有错误
C. 只要攻击者入侵蜜罐的某项服务，系统就会记录下它们的行为并观察它们接下来的所有动作
D. 蜜罐系统拖延攻击者对真正目标的攻击

二、填空题（每空 2 分，共 40 分）

1. RSA算法的安全是基于________的困难。

2. 公开密钥加密算法的用途主要包括两个方面：________；________。

3. 消息认证是________，即验证数据在传送和存储过程中是否被篡改、重放或延迟等。

4. Hash函数是可接受________数据输入，并生成________数据输出的函数。

5. ________是笔迹签名的模拟，是一种包括防止源点或终点否认的认证技术。

6. 身份认证是验证________，而不是冒充的，包括信源、信宿等的认证和识别。

7. ________的目的是为了限制访问主体对访问客体的访问权限。

8. P2DR的含义是：________、________、________和________。

9. IDEA（International Data Encryption Algorithm）是旅居瑞士的中国青年学者来学嘉和著名密钥专家J.Massey于1990年提出，又于1992年改进后形成的，国际上普遍认为它是继DES之后又一成功的分组密码，已经实际应用于E-mail加密系统PGP和许多其他加密系统中。
IDEA是分组密码，明文和密文分组长度均为________位。与DES不同的是，其密钥长度为________位。IDEA与其他分组密码一样，在设计上既采用了混淆，又采用了扩散，混合运用了3个不同的代数群，获得了良好的非线性，增强了密码的安全性。IDEA算法是对合算法，加解密共用同一算法。无论是用软件，还是用硬件，都很容易实现，而且加解密速度很快。

10. 防火墙有许多种形式，按技术划分，防火墙可以分为________、________、电路级网关和________。

11. PHP——Hypertext Preprocessor，是一种易于学习和使用的服务器端HTML嵌入式脚本描述语言，是生成动态网页的工具之一。PHP独特的语法混合了C、Java、Perl以及PHP自创的新语法，其目标是让Web程序员快速地开发出动态的网页。与ASP、JSP一样，PHP也可以结合________共同使用，它与HTML具有非常好的________，使用者可以直接在脚本代码中加入HTML标签，或者在HTML标签中加入脚本代码，从而更好地实现页面控制，提供更加丰富的功能。PHP是完全免费的，它支持几乎所有流行的数据库及操作系统，兼容性强，扩展性强。

三、计算题（共 20 分）

1. 设通信双方使用 RSA 加密体制，接收方的公开密钥是$(e, n)=(5, 35)$，求明文 $M=30$ 对应的密文。（5 分）

2. 假定允许使用 26 个小写字母和 10 个数字构造口令，口令长度为 8 个字符，若采用暴力攻击，在下列情况下各需要多少时间（精确到小数点后 4 位即可）？（1）检查一个口令需要 1/10s 时间。（2）检查一个口令需要 1ns 时间。（7 分）

3. 设明文 *M*= thank you，密钥 *K*=test，则采用维吉尼亚密码的加密字母是什么？十六进制 ASCII 编码输出是什么？（8 分）

维吉尼亚编码规则为给出密钥 $K=k[1]k[2]\cdots k[n]$，若明文为 $M=m[1]m[2]\cdots m[n]$，则对应的密文为 $C=C[1]C[2]\cdots C[n]$，其中，$C[i]=(m[i]+k[i])$ mod 26。维吉尼亚方阵如下所示。

明文	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
…																										
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
…																										
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
…																										
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

四、简答题（20 分）

1. 可以采用哪些技术防御网络嗅探？（5 分）

2. 请详细说明下列程序中是否存在缓冲区溢出？（5 分）

```
/ * File heap1.c * /
# include < stdio.h >
# include < stdlib.h >
# include < unistd.h >
# include < string.h >
# define BUFFER-SIZE 16
# define OVERLAYSIZE 8  /* 我们将覆盖 buf2 的前 OVERLAYSIZE 字节 */
int main()
{
u-long diff;
char * buf1 = (char * ) malloc (BUFFER-SIZE);
char * buf2 = (char * ) malloc (BUFFER-SIZE);
diff = (u-long) buf2 - (u-long) buf1;
printf ("buf1 = %p , buf2 = %p , diff = 0x %x ( %d) bytes \n", buf1, buf2, diff, diff);
/* 将 buf2 用'a'填充 */
memset (buf2, 'a', BUFFER-SIZE - 1), buf2[BUFFER-SIZE - 1 ] = '\0';
printf ("before overflow: buf2 = %s \n", buf2);
/* 用 diff + OVERLAYSIZE 个'b'填充 buf1 */
memset (buf1 , 'b', (u-int) (diff + OVERLAYSIZE));
```

```
printf ("after overflow: buf2 = %s \n", buf2);
return 0 ;
}
```

3. 什么是 X.509 方案，它是如何实现数字签名的？（5 分）

4. 请说明虚拟专用网的定义和关键技术。（5 分）

综合考题二答案

一、1．A　2．D　3．C　4．D　5．D　6．C　7．C　8．A　9．D　10．B

二、

1. 分解两个大素数的积；
2. 密钥分配、数字签名；
3. 验证信息的完整性；
4. 变长，定长；
5. 数字签名；
6. 信息发送者的真实性；
7. 访问控制；
8. 策略，保护，探测，反应；
9. 64，128；
10. 包过滤防火墙、代理服务器型防火墙、混合型防火墙；
11. HTML，兼容性。

三、

1. 接收方的公开密钥是(e, n)=(5,35)，明文M=30 经过加密后为C=30^5 mod 35 =24300000 mod 35 =25，即对应的密文为C=25。

2. 可能产生口令长度为 6 的口令总数量为 36×36×36×36×36×36=2.1767×10^9个，因此如果检查一个口令的时间为 1/10s 时，暴力攻击穷举搜索最长结束时间为 2.1767×10^8s，相当于 3627971min，也就是 60466h，等于 2519 天，相当于 6.9 年的时间。

如果检查一个口令需要 1ns 时间，也就是前面单位时间的 10e(−5)，则穷举搜索完毕需要 36.3min。

3. 加密字母是 MLSG DCGN，十六进制 ASCII 编码输出是 4D 4C 53 47 44 43 47 4E。

四、

1. 网络嗅探的防御通用策略包括采用安全的网络拓扑结构、会话加密技术和防止 ARP 欺骗等方面。此外，也可以借助一些反监听工具（如 Anti Sniffer 等）进行检测。在共享式网络下，嗅探器需要将网卡设置为混杂模式才能工作，因此可以通过检测混杂模式网卡检测可能存在的嗅探器。也可以通过检测网络通信丢包率和网络带宽异常检测网络中可能存

在的嗅探。目前已经有一些检测网络嗅探的手段和方法，如网络和主机响应时间测试和ARP 检测等。交换网络下防范监听的措施主要包括：

① 不要把网络安全信任关系建立在单一的 IP 或 MAC 基础上，理想的关系应该建立在IP-MAC 对应关系的基础上。

② 使用静态的 ARP 或者 IP-MAC 对应表代替动态的 ARP 或者 IP-MAC 对应表，禁止自动更新，使用手动更新。

③ 定期检查 ARP 请求，使用 ARP 监视工具（如 ARPWatch 等）监视并探测 ARP 欺骗。

对于防范网络嗅探攻击，管理显得格外重要。管理部门应建立一套安全标准，严格执行。

2. 存在缓冲区溢出。buf2 的前 8 字节被覆盖了，这是因为向 buf1 中填写的数据超出它的边界进入 buf2 的范围。由于 buf2 的数据仍然在有效的 Heap 区内，所以程序仍然可以正常结束。

虽然 buf1 和 buf2 是相继分配的，但它们并不是紧挨的，而是有 8 字节的间距。这是因为，使用 malloc()动态分配内存时，系统向用户返回一个内存地址，实际上，在这个地址前面通常还有 8 字节的内部结构，用来记录分配的块长度、上一个堆的字节数以及一些标志等。这个间距可能随不同的系统环境而不同。buf1 溢出后，buf2 的前 8 字节也被改写为bbbbbbbb，buf2 内部的部分内容也被修改为 b。

buf1　　　　间距　　　　buf2

覆盖前: [xxxxxxxxxxxxxxxx] [xxxxxxxx] [aaaaaaaaaaaaaaa]

低址 ------------------------------> 高址

覆盖后: [bbbbbbbbbbbbbbbb] [bbbbbbbb] [bbbbbbbbaaaaaaa]

3. X.509 是一种行业标准或者行业解决方案——X.509 公共密钥证书。在 X.509 方案中，默认的加密体制是公钥密码体制。

为进行身份认证，X.509 标准及公共密钥加密系统提供了数字签名的方案。用户可生成一段信息及其摘要（指纹）。用户用专用密钥对摘要加密，以形成签名，接收者用发送者的公共密钥对签名解密，并将之与收到的信息“指纹”进行比较，以确定其真实性。

4. 虚拟专用网（简称 VPN）是利用接入服务器、路由器及 VPN 专用设备、采用隧道技术以及加密、身份认证等方法，在公用的广域网（包括 Internet、公用电话网、帧中继网及 ATM 等）上构建专用网络的技术，在虚拟网上, 数据通过安全的“加密隧道”在公众网络上传播。

VPN 使用的主要技术包括：

（1）隧道（封装）技术是目前实现不同 VPN 用户业务区分的基本方式。一个 VPN 可抽象为一个没有自环的连通图，每个顶点代表一个 VPN 端点（用户数据进入或离开 VPN的设备端口），相邻顶点之间的边表示连接这两对应端点的逻辑通道，即隧道。隧道以叠加在 IP 主干网上的方式运行。需安全传输的数据分组经一定的封装处理，从信源的一个 VPN

端点进入 VPN，经相关隧道穿越 VPN（物理上穿越不安全的互联网），到达信宿的另一个 VPN 端点，再经过相应解封装处理，便得到原始数据。(不仅指定传送的路径，在中转节点也不会解析原始数据)

（2）当用户数据需要跨越多个运营商的网络，在连接两个独立网络的节点时，该用户的数据分组需要被解封装和再次封装，可能会造成数据泄露，这就需要用到加密技术和密钥管理技术。目前主要的密钥交换和管理标准有 SKIP 和 ISAKMP（安全联盟和密钥管理协议）。

（3）对于支持远程接入或动态建立隧道的 VPN，在隧道建立前需要确认访问者身份，是否可以建立要求的隧道，若可以，系统还须根据访问者身份实施资源访问控制。这需要访问者与设备的身份认证技术和访问控制技术。

参 考 文 献

[1] 张基温. 信息系统安全教程[M]. 3 版. 北京：清华大学出版社，2017.

[2] 张玉清. 网络攻击与防御技术[M]. 北京：清华大学出版社，2011.

[3] 张玉清. 网络攻击与防御技术实验教程[M]. 北京：清华大学出版社，2010.

[4] 张玉清，王凯，杨欢，等. Android 安全综述[J]. 计算机研究与发展，2014，51（7）：1385-1396.

[5] 何敏. 计算机病毒探测技术研究[J]. 计算机知识，2016（8）：39-40.

[6] 沈继涛. 计算机网络安全防范策略[J]. 电子技术与软件工程，2017，209-210.

[7] 马铮，张小梅，夏俊杰，等. 基于 SDN 技术的 DDoS 防御系统简析[J]. 邮电设计技术，2016（1）：55-59.

[8] 刘建伟，刘培顺，赵波，等. 信息系统安全实验教程[M]. 北京：清华大学出版社，2012.

[9] 凯文·米特尼克. 入侵的艺术[M]. 北京：清华大学出版社，2007.

[10] 凯文·米特尼克. 反欺骗的艺术[M]. 北京：清华大学出版社，2014.

[11] Zheng J, Li Q, Gu G, et al. Realtime DDoS defense using COTS SDN switches via adaptive correlation analysis[J]. IEEE Transactions on Information Forensics and Security, 2018，13(7): 19 -22.

[12] 陈禹，张敏钰. 电话监听的秘密世界[J]. 保密科学技术，2011（7）：73-74.

[13] 史惠中. 网络安全技术和黑客攻击技术关系辨析[J]. 电子技术与软件工程，2016（1）：218.

[14] 吴彬. 计算机信息安全保密的技术研究[J]. 信息技术与应用，2017（1）：171-172.

[15] 李可，方滨兴，崔翔，等. 僵尸网络发展研究[J]. 计算机研究与发展，2016（10）：2189-2206.

[16] 李龙谱，斯雪明，张志鸿，等. 在多 FPGA 上实现基于字典的 ZIP 文档口令恢复[J]. 计算机应用与软件，2015（6）：292-295.

[17] 徐宁，杨庚. 基于身份加密机制的光学加密密钥系统[J]. 通信学报，2012（4）：121-128.

[18] 戚娜. 数字水印的相关应用研究[J]. 电子设计工程，2017（1）：152-154.

[19] 阳溢，刘博文，张文静. 信息隐藏技术在大数据环境中的应用探讨[J]. 计算机编程技巧与维护，2017（17）：62-65.

[20] 王大印，林东岱，吴文玲，等. XOR-MAC 消息认证码的安全性新证明[J]. 中国科学院研究生院学报，2006（3）：257-262.

[21] 张小刚. 电子商务中 SET 协议安全技术浅析[J]. 商场现代化，2008（11）：130-131.

[22] 殷媛. 加密技术在通讯安全中的运用[J]. 通信设计与应用，2017（3）：137.

[23] 刘金会，张焕国，贾建卫，等. HKKS 密钥交换协议分析[J]. 计算机学报，2016（3）：516-528.

[24] 陈宇航，贾徽徽，姜丽莹，等. 基于 Grover 算法的 ECC 扫描式攻击[J]. 技术研究，2016（2）：28-33.

[25] 张弢. 基于 LabVIEW 的以太网数据监听与通信分析[J]. 信息通信，2015（8）：198-201.

[26] 黄文，文春生，欧红星. ICMP 路由欺骗与 ARP 欺骗研究[J]. 湖南科技学院学报，2005（12）：49-57.

[27] 罗靖玮，肖昌兴. PKI 在电子信息安全中的应用研究[J]. 信息通信，2017（7）：171-172.

[28] 李宁，吴耀华. 基于 X. 509 的双向认证框架[J]. 计算机工程与应用，2005（8）：157-161.

[29] 李胜广，杨东凯，刘建伟. 防火墙及网络协议综合实验平台构建[J]. 实验技术与管理，2007（2）：72-76.

[30] 毕凯，周炜. 基于蜜罐的安全系统设计[J]. 计算机工程与设计，2010（22）：4806-4810.

[31] 赵凯. 网络诱骗的基本原理、要求及应用分析[J]. 信息通信，2012（5）：133-136.

[32] 张婷婷，夏戈明，吴伟彬. 安全与应急响应的监测型移动传感器网络系统[J]. 技术研究，2013（11）：26-30.
[33] James Michael Stewart,Mike Chappie,Darril Gibs. CISSP 认证考试指南[M]. 7 版. 唐俊飞，陈峻，译. 北京：清华大学出版社，2017.
[34] GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南[P]. 北京：中国标准出版社，2015.
[35] 吴世忠，等. 信息安全保障[M]. 北京：机械工业出版社，2014.
[36] 吴世忠，等. 信息安全技术[M]. 北京：机械工业出版社，2014.
[37] 李潇，刘俊奇，范明翔. WannaCry 勒索病毒预防及应对策略研究[J]. 电脑知识与技术，2017（19）：19-20.

后　　记

在本书的编写过程中，查阅了网上的丰富资源，得益于很多网络技巧和窍门的无私分享，感谢网络世界默默无闻的众多奉献者，使得网络在高开放性的同时，还能保持高度的可靠性和安全性。同时，本书的编写也得到很多前辈、同事以及学生的帮忙，家人也给予了我们无微不至的关怀。在本书的编写过程中，第一作者的父亲不幸离世，也借此书慰藉他的灵魂。梦一样易逝的人生需要我们坚强面对。希望这个世界永远安全，没有纷争。

高等教育质量工程信息技术系列示范教材

系列主编：张基温

- 新概念 C 程序设计大学教程（第 4 版） 张基温
- 新概念 C++程序设计大学教程（第 3 版） 张基温
- 新概念 Java 程序设计大学教程（第 3 版） 张基温
- 计算机组成原理教程（第 7 版） 张基温
- 计算机组成原理解题参考（第 7 版） 张基温
- 计算机网络教程（第 2 版） 张基温
- 信息系统安全教程（第 3 版） 张基温
- 信息系统安全教程（第 3 版）习题详解 栾英姿
- Python 大学教程 张基温
- 大学计算机——计算思维导论 张基温
- UI 设计教程 牛金巍
- APP 开发教程——HTML5 应用 尹志军